Oracle® Communications

Service Communication Proxy (SCP) Cloud Native User's Guide

Release 1.7.5.1
F32456-05
December 2020

Oracle Communications Service Communication Proxy (SCP) Cloud Native User's Guide, Release 1.7.5.1

F32456-05

Copyright © 2019, 2020, Oracle and/or its affiliates.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software" or "commercial computer software documentation" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government’s use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Contents

List of Figures

List of Tables

My Oracle Support

My Oracle Support (https://support.oracle.com) is your initial point of contact for all product support and training needs. A representative at Customer Access Support can assist you with My Oracle Support registration.

Call the Customer Access Support main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. When calling, make the selections in the sequence shown below on the Support telephone menu:

1. Select **2** for New Service Request.
2. Select **3** for Hardware, Networking and Solaris Operating System Support.
3. Select one of the following options:
    - For Technical issues such as creating a new Service Request (SR), select **1**.
    - For Non-technical issues such as registration or assistance with My Oracle Support, select **2**.

You are connected to a live agent who can assist you with My Oracle Support registration and opening a support ticket.

My Oracle Support is available 24 hours a day, 7 days a week, 365 days a year.

Whats New in This Guide

This section introduces the documentation updates for Release 1.7.x in Oracle Communications Cloud Native Service Communication Proxy (SCP) User's Guide.

Release 1.7.5.1

For Release 1.7.5.1, the following change is performed in this document:

- SCPIngressGatewayPodMemoryUsage is added in Alerts section.

Release 1.7.5

For Release 1.7.5, the following changes are performed in this document:

- New metrics are added to calculate NF wide rate, refer to Metrics Reference for more information::
  - ocscp_metric_nf_total_http_tx_req
  - ocscp_metric_nf_total_http_rx_req
  - ocscp_metric_nf_total_http_rx_res
  - ocscp_metric_nf_total_http_tx_res
  - ocscp_metric_nf_total_http_rx_res_xx
  - ocscp_metric_nf_total_http_tx_res_xx
- Alerts/Alarms are updated as follows in Alerts section:
  - Expressions updated with correct labels:
    - SCPSoothsayerNotificationPodMemoryUsage
    - SCPWorkerPodMemoryUsage
    - SCPPilotPodMemoryUsage
    - NFInstanceConnectionDown
  - Expression modified to use different function:
    - SCPInstanceDown

Refer to SCP User's Guide for more information.

Release 1.7.2

For Release 1.7.2, the following changes are performed in this document:

- Added the following metrics, refer to Metrics Reference for more information:
  - ocscp_metric_downstream_request_reset
  - ocscp_metric_scp_generated_response
  - ocscp_metric_config_error_cluster_not_found

Release 1.7.0

For Release 1.7.0, the following changes are performed in this document:

- Added the following parameters:

  - cbEnabled: Refer to Configuring SystemOptions and Configuring Circuit Breaking and Outlier Detection for more information.
  - odEnabled: Refer to Configuring SystemOptions and Configuring Circuit Breaking and Outlier Detection for more information.
  - DB Lookup Error: Refer to Configuring Routing Options for more information.
- Added the following metrics, refer to Metrics Reference for more information:
  - scp_soothsayer_nrf_registration_success_total
  - scp_soothsayer_nrf_registration_failure_total
  - scp_soothsayer_nrf_heartbeat_success_total
  - scp_soothsayer_nrf_heartbeat_failures_total
  - ocscp_metric_upstream_service_time
  - ocscp_metric_request_header_to_body_time
  - ocscp_metric_request_complete_time
  - ocscp_metric_downstream_connection
  - ocscp_metric_total_http_rx_downstream_req
  - scp_soothsayer_mediation_total_rules_per_trigger
  - ocscp_upstream_app_service_time_ms
- Updated Configuring Mediation Options section.
- Added new alerts related to mediation operation in Alerts section.

1 Introduction

This document provides information on how to use the Oracle Communications Service Communication Proxy (SCP) in the cloud native 5G core network.

The core network in 5G follows a Service Based Architecture where network functions advertise and provide services that can be consumed using REST APIs by other functions. This allows for the adoption of web-scale technologies and software that are used by different organizations in telecom networks.

The SCP provides other 5G Network Functions the following functionalities:

- **Routing/Selection**: Routing rules, refresh cache, and handle application failures/ redirects.
  - **Dynamic Discovery**: 5G Topology is dynamically determined from the NRF and creation of routing rules.
  - **Static Configuration**: Enables configuring NF Profiles statically.
- **Load Balancing**: Load balancing based on static capacity, NF-Type, NF-specific and NF Priority mentioned in NF Profile.
- **NF Subscription**: Subscription for all NF types.
- **Circuit Breaking**: Trigerred on a per FQDN basis when outstanding transactions exceeds a configurable value.
- **Message Priority** : Message Priority assignment/override based on the 3gpp-Sbi-Message-Priority header.
- **Congestion and Overload**: Uniform load balancing/routing strategy across the network and protects the pod (server) from overload with respect to various system resources

Acronyms and Terminologies

The following table provides information about the acronyms and terminologies used in the document.

Table 1-1 Acronyms and Terminologies

Field	Description
3GPP	3rd Generation Partnership Project
5GC	5G Core Network
5GS	5G System
AF	Application Function
AUSF	Authentication Server Function
BSF	Binding Support Function
CHF	Charging Function
CNE	Cloud Native Environment

Table 1-1 (Cont.) Acronyms and Terminologies

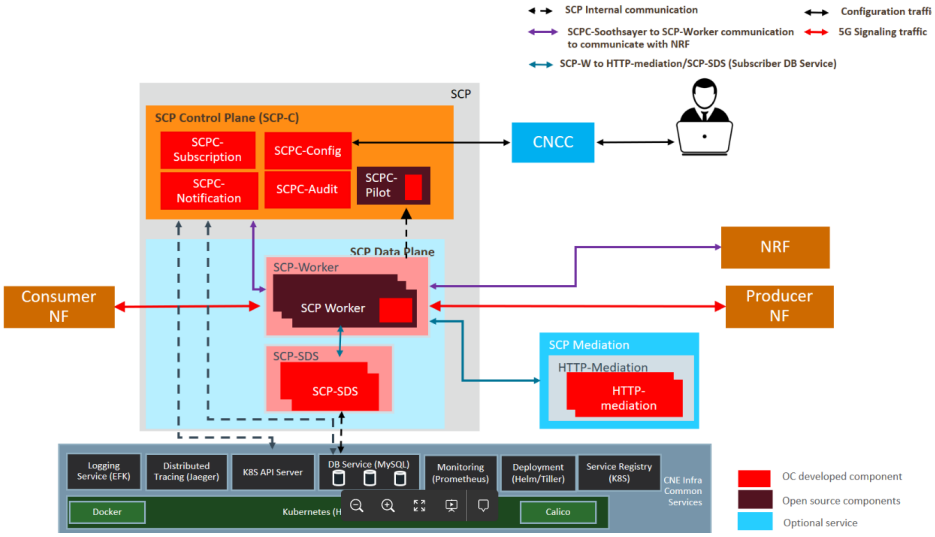
Field	Description
EFK stack	Elasticsearch, Fluentd, and Kibana stack
FQDN	Fully Qualified Domain Name
GPSI	Generic Public Subscription Identifier
IWF	InterWorking and Mediation Function
K8s	Kubernetes
NEF	Network Exposure Function
NF	Network Function
NRF	Network Repository Function
NSSF	Network Slice Selection Function
PCF	Policy Control Function
PFD	Packet Flow Description
QFI	QoS Flow Identifier
QoE	Quality of Experience
SBA	Service Based Architecture
SBI	Service Based Interface
SCP	Service Communication Proxy
SCPC	Service Communication Proxy Control
SEPP	Security Edge Protection Proxy
SMF	Session Management Function
SUPI	Subscription Permanent Identifier
UDR	Unified Data Repository
UDSF	Unstructured Data Storage Function

2
Service Communication Proxy Architecture

This section explains the Service Communication Proxy system architecture.

The Service Communication Proxy is a decentralized solution and composed of control plane and data plane. This solution is deployed along side of 5G Network Functions (NF) for providing routing control, resiliency, and observability to the core network.

Figure 2-1 Service Communication Proxy Architecture



> **Note:**
>
> SCP SDS App service is optional component.

The Service Communication Proxy solution is deployed either as a default outbound proxy to NF instances or as a router model where SCP is configured as http2 outbound proxy at each NFs in cloud native environments. SCP provides the following benefits to the 5G core network architecture:

Improved Load Balancing

The 5G core network is a service based architecture which does not lend itself to an efficient load balancing of provider NFs and by introducing a Service Communication Proxy in the midst, load balancing across available NFs can be significantly improved. The Service Communication Proxy has a complete view of all the messages arriving for a given NF type and supports traffic distribution schemes such as round robin based on capacity and its availability.

Routing Control

Service Communication Proxy provides better routing control and bring resiliency to the network. It relieves user NFs from remembering and interpreting complex routing rules associated with next hop selection and at the same time makes re-routing decisions based on load conditions and health status of NF providers within configuration time-period.

In the absence of an alternate route, the Service Communication Proxy rejects requests destined to a failed or degraded NF, thereby acting as a circuit breaker. This prevents valuable resources at the user NFs from being tied up waiting for responses from providers. The Service Communication Proxy retries on behalf of the service user there by relieving the service user from this burden and leaving it to focus on the application.

Message Priority Assignment/Override

3gpp-Sbi-Message-Priority header is defined to carry the message priority of 5G messages. The SCP includes or modifies the header based on the configuration parameters. See Configuring MessagePriority Options.

Circuit Breaking and Outlier Detection

Service Communication Proxy tracks the status of each individual endpoint of the producer NFs/NF Services. Upstream producer EndPoints that continually return 5xx errors for service requests are ejected from the routing pool for a pre-defined period of time. Outlier detection is a form of passive health checking of producer NFs. Outlier detection is per endpoint (of producer NF instance) and triggers when SCP receives consecutively 5xx error response and exceeds the configurable number of consecutive 5xx errors.
Circuit breaking is triggered on a per FQDN basis when its outstanding transactions exceeds a configurable value. When circuit breaking is activated, requests are alternate routed if possible or rejected.

Overload Control

The overload control protects the pod (server) from overload with respect to various system resources such as memory, CPU, or file descriptors due to several client connections or requests.

The SCP worker supports overload control based on the usage of the memory.

The SCP worker considers itself to be overloaded if the usage associated with memory exceeds the operator configured threshold values.

In the event of overload, the SCP performs the below configured actions:

- Refuse new connections
- Respond to new ingress requests with a configurable Error (http status) and code (Default Error code - 503).

Observability

The following are available in observability.

- **Metrics**

Metrics services requests are proxied through the Service Communication Proxy, the Service Proxy Controller collects Metrics and KPIs related to message processing. With this information, the Service Communication Proxy is in a unique position to provide a view of health status the network at a given time. See Alerts, Metrics and Traces.

- **Tracing**
  Compliant with open API tracing
- **Logging**
  Compliant with EFK stack

Static Configuration

Static configuration fallback feature provides static configuration of NF profiles when geo-redundant NRFs in the network fails. Under normal conditions, SCP learns the 5G topology from NRF and uses it for creating the routing rules. Under failure conditions or when NRF is not configured or when static configurable routing is preferred, SCP uses the user configured/updated NF profiles. SCP retains the 5G topology info from NRF for further operations. It allows fallback to a static mode of operation for modifying the previously discovered NF Producers profiles (via NRF) as well as add any new NF Producer profiles while the NRFs are still unavailable. The following configurations are used for static configuration fallback feature:

- **TopologySourceInfo** - This is the configuration which is used by SCP to determine the 5G topology source. SCP learns and creates the routing rules accordingly.
- **5G NF topology Info** - This is the information available at the SCP after learning the 5G topology from the defined source as per previous section configuration (either from NRF or static method).
- User can create/get/update/delete the 5G NF Profile information.

SCP Microservices

Following is the list of SCP microservices:

Table 2-1 SCP Microservices

Microservices	Description
SCPC-Pilot	SCPC-Pilot keep track on Service registry and CRDs for any change and updates the route rules/configuration and translates them into low-level Envoy configuration & provide to Worker, when requested
SCPC-Notification	It configures routing rules as per 5G NF topology information gathered from NRF or as result of Audit.
SCPC-Audit	it does periodic audit with NRF to synchronize the 5G NF topology information and updates routing rules via notification, if needed.
SCPC-Config	It provides configuration interface for SCP configuration.
SCPC-Subscription	It performs NRF management and NRF discovery service operation for SCP registration and subscription for NF change notification.
SCP-Worker	SCP-Worker receives 5G signaling traffic and controls communication/routing between 5G NFs/Services.

Table 2-1 (Cont.) SCP Microservices

Microservices	Description
SCP-SDS (optional)	Subscriber Data/DB Service, which maintains the serving AMF and SMF info for an UE.

3 Configuring Service Communication Proxy using REST APIs

This section provides information for configuring Service Communication Proxy using REST APIs.

SCP provides the following two service interfaces:

- **Signaling Interface**
  - Signaling interface is exposed by SCP data plane (that is, SCP Worker) and this interface will be used to receive all 5G signaling traffic.
- **Config Interface**
  - Config interface is exposed by SCP control plane (that is, SCPC-Config) and this interface is used to receive all SCP configuration traffic.

SCP Signaling Service

- **FQDN**
  - Consumer NFs may use SCP Signaling service's FQDN to send the 5G signaling traffic to SCP for routing.
  - K8S service FQDN will be in the form as below:
    * fqdn = scp-worker.<namespace>.<domain> where, namespace is K8S namespace as provided during helm installation, and domain is as provided in helm chart (values.yaml) while installation.
    * If user NFs are deployed outside of K8S cluster, then operator needs to make sure that this fqdn is resolvable by consumer NFs.
    * Operator can specify the public or K8s-cluster fqdn of SCP in helm chart (values.yaml, scpInfo.fqdn" = <releaseName>-scp-worker.<Namespace>.<domain>) during installation.
- **IP Address**
  - Consumer NFs may use SCP Signaling service's IP Address to send the 5G signaling traffic to SCP for routing.
  - <global.publicSignalingIP>, as provided in helm chart (values.yaml) while installation.

> **Note:**
>
> Only IPv4 is supported.

- **Port**
  - Consumer NFs need port information along with fqdn/ip address to send the 5G signaling traffic to SCP for routing.

  - Port is <global.publicSignalingPort> as provided in helm chart (values.yaml) while SCP installation.

SCP Config Service

- **FQDN**
  - Operator may use SCP Config service's FQDN to configure the SCP for routing.
  - K8s service FQDN will be of the form as below:
    * fqdn = scpc-config-svc.<namespace>.<domain> where, namespace is K8s namespace as provided during helm installation, and domain is as provided in helm chart (values.yaml) while installation.
    * Operator need to make sure that this fqdn is resolvable, if operating from outside of K8S cluster.
- **IP Address**
  - Consumer NFs may use SCP Config service's IP Address to configure the SCP for routing.
  - <scpc-soothsayer.configService.publicConfigIP>, as provided in helm chart (values.yaml) while installation.
- **Port**
  - Operator needs port information along with fqdn/ip address to configure the SCP for routing.
  - Port is 8081 that is a fixed port (not configurable).

Configuring CanaryRelease Options

The CanaryRelease inspects the version (API version) attribute of the NF Service profile published by the NFs (during NF registration/update) and can identify the release as a canary version if the version matches the configured value. There are two versions of API, Production version that is older version and Canary version that is the newer version of the service instance. The SCP distributes traffic between Production version and the Canary versions based on operator configuration.

User can configure CanaryRelease options. The supported operations are **LIST**, **GET**, and **PATCH**.
Following REST message samples provide the details about the operations and parameters for CanarayRelease Options. The default values of parameters related to CanaryRelease are mentioned in the following samples, however, user can modify these values. These parameters are applicable at POD level.

REST Message Samples

Request_Type: GET
URL: */soothsayer/v1/ canaryrelease/*

Port: 8081

Message

```
[{
"canaryReleaseFlag": false,
```

```
"serviceName": "nudm-uecm"
"apiFullVersion": "1.R15.1.0",
"canaryTraffic": 5
}
...
]
```

Example:

```
curl --header 'Content-type: application/json' --header 'accept:
application/ json' --request GET http://<SCP config service fqdn>:8081/
soothsayer/v1/ canaryrelease/

[{

  "canaryReleaseFlag": false,

  "serviceName": "nudm-uecm",

  "apiFullVersion": "2.R16.1.0",

  "canaryTraffic": 5

}

...

]
```

Request_Type: LIST
Message

```
curl --header 'Content-type: application/json' --header 'accept:
application/json' --request GET http://<SCP config service fqdn>:8081/
soothsayer/v1/canaryrelease/

[{
  "canaryReleaseFlag": false,
  "serviceName": "nudm-uecm",
  "apiFullVersion": "2.R16.1.0",
  "canaryTraffic": 5
}
...
]
```

Request_Type: PATCH
Field Name and Type: canaryReleaseFlag <Boolean>

Description: Enable/Disable canary release support. Set the value of field canaryReleaseFlag and mention serviceName for which the configuration is needed in the resource path of below Curl Command.

Default Value: null

Message:**canaryReleaseFlag UPDATE Command**

```
curl --header "Content-Type: application/json" --request PATCH --data '{
      "canaryReleaseFlag": true
}' http://<SCP config service fqdn>:8081/soothsayer/v1/canaryrelease/
<serviceName>
```

Request_Type: PATCH
Field Name and Type: apiFullVersion <String>

Description: The API full version of the canary service. Set the value of field apiFullVersion and mention serviceName for which the configuration is needed in the resource path of below Curl Command.

Default Value: null

Message: **apiFullVersion UPDATE Command**

```
curl --header "Content-Type: application/json" --request PATCH --data '{
        "apiFullVersion": "2.R16.1.0"
}' http://<SCP config service fqdn>:8081/soothsayer/v1/canaryrelease/
<serviceName>
```

Request_Type: PATCH
Field Name and Type: canaryTraffic <Integer>

Description: The traffic that should be distributed to Canary release. Set the value of field canaryTraffic and mention serviceName for which the configuration is needed in the resource path of below Curl Command.

Default Value: null

Message: **canaryTraffic UPDATE Command**

```
curl --header "Content-Type: application/json" --request PATCH --data '{
       "canaryTraffic": 10
}' http://<SCP config service fqdn>:8081/soothsayer/v1/canaryrelease/
<serviceName>
```

Configuring Routing Options

SCP acts as a proxy and forwards or routes any 5G ingress service request to the host (5G NF) present in the request's URI.

SCP supports:

- Routing based on IMSI and MSISDN only.
  - Routing based on SUPI and GPSI is supported based on the start and end attributes only as published in NFProfile and routing based on the pattern attribute is not supported.
- Only IPv4 IP family.
- Every producer NFs are required to publish IpEndPoints for each NFServices in NFProfile while registering with NRF.

- Routing Scope: Site
- DB Sync Status: No Sync, Site Wide
  - Load Balancing and alternate routing is based on DB Sync Status within Site.
- Load Balancing Algorithm: Priority only (and capacity).
  - Load Balancing across the equivalent NFs/NF Services is based on priority and capacity.

Types of routing options

The types of routing options are:

- Pod Level Routing Options: Controls routing across the pods of selected NF.
- Service Level Routing Options: Controls routing of selected NF services.

Parameters for Configuring Routing Options

Table 3-1 provide details of the parameters for configuring Routing Options.

Table 3-1 Parameters for RoutingOptions

Parameter Name	Description	Applicable to NF Service Level	Default Values	Value Range	Applicable to Pod level within NF	Values
Response Timeout	When response timeout expires, then SCP initiates alternate rerouting to available alternate NF or Pod.	Yes	1000 ms	100-10000 ms	Yes	1 s Supported values can be in 's' or 'ms', where 's' is seconds and 'ms' is milliseconds.
Total transaction lifetime	• Time consumed in processing of all retries should not exceed the total transaction life time. • The total time allowed to forward a request, including initial and all subsequent routing attempts	Yes	6 seconds	100 - 240000	Yes	6 seconds

Table 3-1 (Cont.) Parameters for RoutingOptions

Parameter Name	Description	Applicable to NF Service Level	Default Values	Value Range	Applicable to Pod level within NF	Values
Max Routing attempts	• Number of re-route attempt (retries) at NF/Pod level • Maximum number of times SCP is allowed to forward a request message. If the Max Routing attempts value is set to 1 for both Service and Pod level, the total transaction lifetime field value is not needed and If the Max Routing attempts value (including both service and pod level) is greater than 1, total transaction lifetime value is considered in rerouting processing.	Yes	3	1-5	Yes	2

Table 3-1 (Cont.) Parameters for RoutingOptions

Parameter Name	Description	Applicable to NF Service Level	Default Values	Value Range	Applicable to Pod level within NF	Values
Reroute on Response Code	• SCP will attempt a reroute if the upstream server responds with any of these configured response code. – 5xx (includes gateway-error, connection-failure, refused-stream) – 500 (Internal Server Error) – 501 (Not Implemented) – gateway-error (502, 503, 504) – 404 (Not Found) – 408 (Request Timeout) – retriable-4xx (409) – 410 (Gone) – 307 (Temporary Redirect) – 308 (Permanent Redirect) • SCP attempts re-route the request in case of response timeout, connect-failure, refused-stream, GOAWAY frame received on any connection. These options (events) are not configurable and is supported by SCP.	5xx, which includes gateway-error (502, 503, 504.) connect-failure, refused-stream. retriable-4xx (409)	-			-
Actions	Supported actions • Forward the ingress service request to selected egress producer NF • Send Response with configured result code and message. • Abandon or drop the ingress service request	Yes	Forward			

Table 3-1 (Cont.) Parameters for RoutingOptions

Parameter Name	Description	Applicable to NF Service Level	Default Values	Value Range	Applicable to Pod level within NF	Values
Load Balancing Algorithm	Priority Only: Use priority as the first level criteria. Use capacity as second level criteria	Yes	Priority Only		Yes	Round Robin
Default Priority	• Priority (relative to other NF Services of the same type) in the range of 0-65535, to be used for NF Service selection; lower values indicate a higher priority. If priority is present in either NF profile or nfServiceList parameters, those will have precedence over this value. • This default priority value shall be used for NF service instance selection only if priority is not published by producer NFs while registration with NRF in NF profile (including both NF profile and nfServiceList parameters).	Yes	1		No	-

Table 3-1 (Cont.) Parameters for RoutingOptions

Parameter Name	Description	Applicable to NF Service Level	Default Values	Value Range	Applicable to Pod level within NF	Values
Default Capacity	• Capacity information in the range of 0-65535, expressed as a weight relative to other NF service instances of the same type; if capacity is also present in either NF profile or nfServiceList parameters, those will have precedence over this value. • This default capacity value shall be used for NF service instance selection only if capacity is not published by producer NFs while registration with NRF in NF profile (including both NF profile and nfServiceList parameters).	Yes	65535		No	-
reverseProxySupport	Flag used to enable reverse proxy support for a service. In reverse proxy mode all the requests will have authority as SCP. SCP will forward those requests to respective Producers after making required authority changes in the requests (both initial and subsequent). Currently reverse proxy mode is supported only for some interfaces. If the flag is set to false then transparent proxy mode is enabled. If reverseProxySupport flag is set to true then it will supersede the initialServiceRequest.routePolicy irrespective if it is set to 'Forward_Route' and create rules for initial messages in Load_balance way.	Yes	false		No	true, false

Table 3-1 (Cont.) Parameters for RoutingOptions

Parameter Name	Description	Applicable to NF Service Level	Default Values	Value Range	Applicable to Pod level within NF	Values
Exceptions	Resource Exhausted Action • Action taken when a request cannot be processed due to an internal resource being exhausted. • Options: – Abandon with no Answer – Send Answer with configured HTTP status code. Refer to HTTP Status Code and applicability for rerouting.	Yes	Abandon with no Answer		No	
	No Producer Response Action • Action taken when the routing of a request is abandoned due to an answer timeout or total transaction lifetime timeout. • Options: – Abandon with no Answer – Send Answer with configured http status code. Refer to HTTP Status Code and applicability for rerouting.	Yes	Send Answer with configured http status code (Default 503).		No	

Table 3-1 (Cont.) Parameters for RoutingOptions

Parameter Name	Description	Applicable to NF Service Level	Default Values	Value Range	Applicable to Pod level within NF	Values
	Connection Failure Action • Action taken when the routing of a request is abandoned when the last egress connection selection fails • Options: – Abandon with no Answer – Send Answer with configured HTTP status code. Refer to HTTP Status Code and applicability for rerouting.	Yes	Send Answer with configured http status code (Default 503).		No	
	Host not found Action • Action taken when the routing of a request is abandoned due to FQDN of the host not found. • Options: – Abandon with no Answer – Send Answer with configured http status code. Refer to HTTP Status Code and applicability for rerouting.	Yes	Send Answer with configured http status code (Default 503).		No	
	DB Lookup Error • Action taken when the routing a Session/ Subscriber binding not found/look-up failure at OCSCP-SDS Service • Options: – Abandon with no Answer – Send Answer with configured http status code. Refer to HTTP Status Code and applicability for rerouting.	Yes	Send Answer with configured http status code (Default 500).		No	

Table 3-1 (Cont.) Parameters for RoutingOptions

Parameter Name	Description	Applicable to NF Service Level	Default Values	Value Range	Applicable to Pod level within NF	Values
reRouteOnResponseCodeList	Reroute on Response Code List: Supported values: ALL_SERVER_ERROR("5xx"), INTERNAL_SERVER_ERROR("500"), NOT_IMPLEMENTED("501"), GATEWAY_ERROR("gateway-error"), CONNECT_FAILURE("connect-failure"), REFUSED_STREAM("refused-stream"), NOT_FOUND("404"), REQUEST_TIMEOUT("408"), RETRIABLE_4XX("retriable-4xx"), GONE("410"), TOO_MANY_REQUESTS("429"), TEMPORARY_REDIRECT("307"), PERMANENT_REDIRECT("308")	No	-		Yes	["ALL_SERVER_ERROR", "NOT_FOUND", "REQUEST_TIMEOUT", "RETRIABLE_4XX", "GONE", "TOO_MANY_REQUESTS", "TEMPORARY_REDIRECT", "PERMANENT_REDIRECT"]

Table 3-1 (Cont.) Parameters for RoutingOptions

Parameter Name	Description	Applicable to NF Service Level	Default Values	Value Range	Applicable to Pod level within NF	Values
nfServiceLoadBasedCongestionControl	NF Service Load Based Congestion Control Rules are updated with new Load as soon as Notification with updated NF profile with updated load is received by SCP and then SCP check rules before routing each request. If SCP is not able to do alternate routing then SCP will forward the message to the NF picked initially that is overloaded NF. In throttling case, it would discard message if not possible to alternate route.	Yes	Default Value: alternateRoutingOnsetThresholdPercent: 80 alternateRoutingAbatementThresholdPercent: 75 throttleOnsetThresholdPercent: 90 throttleAbatementThresholdPercent: 85 responseErrorCode: 503		-	-
deploymentModel	Deployment model of the NF/NF service. • Default, SITE_WIDE is supported for all NF services • REGIONAL deployment is supported only for CHF NF in addition to SITE_WIDE. • Limitation: – PRIMARY_SECONDARY_PAIR deployment is not supported	Yes	SITE_WIDE		Yes	SITE_WIDE
initialServiceRequest	It takes routePolicy and reroutePolicy for initial service request.					

Table 3-1 (Cont.) Parameters for RoutingOptions

Parameter Name	Description	Applicable to NF Service Level	Default Values	Value Range	Applicable to Pod level within NF	Values
subsequentServiceRequest	It takes routePolicy and reroutePolicy for subsequent service request.					

Table 3-2 deploymentCHF

Enumeration value	CHF Deployment
REGIONAL	Regional CHF deployment that is CHFs are deployed in Primary region and Secondary region. A region may consist of one or more locality.
SITE_WIDE	Site specific CHF deployment that is CHF instances are deployed as per SCP's Site deployment.
PRIMARY_SECONDARY_PAIR	Primary and Secondary CHF deployment using ChfServiceInfo. Primary and Secondary CHF instance info is published in ChfServiceInfo while registering with NRF.

Table 3-3 initialServiceRequest

routePolicy	reroutePolicy
Load_Balance	Reroute options • RerouteDisabled • Options in SITE_WIDE deployment – RerouteWithinSite – RerouteAcrossMatedSite – RerouteAcrossNetwork • Options in REGIONAL deployment – RerouteWithinRegion – RerouteAcrossRegion • Options in PRIMARY_SECONDARY_PAIR deployment – RerouteWithinPairGroup
Forward_Route	

Table 3-4 subsequentServiceRequest

routePolicy	reroutePolicy
Load_Balance	Reroute options • RerouteDisabled • Options in SITE_WIDE deployment – RerouteWithinSite – RerouteAcrossMatedSite – RerouteAcrossNetwork • Options in REGIONAL deployment

Table 3-4 (Cont.) subsequentServiceRequest

routePolicy	reroutePolicy
Forward_Route	– RerouteWithinRegion – RerouteAcrossRegion • Options in PRIMARY_SECONDARY_PAIR deployment – RerouteWithinPairGroup

Engineering Configurations

This table defines the min and max ranges for Response Timeout, Max Routing attempts and Total transaction lifetime parameters.

Table 3-5 Engineering Configurations

Name	Type	Attribute	Description
Table_Name	String	Composite Primary Key	Name of the table which will be using this record. Example. ROUTING_OPTIONS
Parameter	String	Composite Primary Key	Name of the engineering configurable parameter. Example. responseTimeOut in ROUTING_OPTIONS
Value	JSON		Value of the engineering configurable parameter. Example: `[{"level": "GLOBAL","type": "RANGE","value": [{"minRange": "1","maxRange": "10","unit": "ms"},{"minRange": 1,"maxRange": 10,"unit": "s"}]}]`

Configuring Operations for Routing Options

User can configure routing options by using the operations **LIST**, **GET**, **PUT** and **PATCH**.

The following sections provide sample details of the operations to configure routing options.

Request_Type: PUT

URL: */soothsayer/v1/routingoptions/*

Port: 8081

Message

```
curl --header 'Content-type: application/json' --header
'accept: application/json' --request GET http://<Soothsayerfqdn>:8081/
soothsayer/v1/routingoptions/<serviceName>
{
  "pod": {
    "maxRoutingAttempts": 1,
    "alternateRouting": false,
```

```
    "loadBalancingAlgorithm": "Round_Robin"
  },
  "srv": {
    "name": "nudm-uecm",
    "maxRoutingAttempts": 3,
    "actions": "Forward",
    "loadBalancingAlgorithm": "Priority_only",
    "nfServiceLoadBasedCongestionControl": {
      "alternateRoutingOnsetThresholdPercent": 80,
      "alternateRoutingAbatementThresholdPercent": 75,
      "throttleOnsetThresholdPercent": 90,
      "throttleAbatementThresholdPercent": 85,
      "responseErrorCode": 503
    },
    "defaultPriority": 1,
    "defaultCapacity": 65535,
    "reverseProxySupport": true,
    "initialServiceRequest": {
      "routePolicy": "Forward_Route",
      "reroutePolicy": "RerouteWithinSite"
    },
    "subsequentServiceRequest": {
      "routePolicy": "Forward_Route",
      "reroutePolicy": "RerouteWithinSite"
    }
  },
  "totalTransactionLifetime": "6s",
  "reRouteOnResponseCodeList": [
    "ALL_SERVER_ERROR",
    "NOT_FOUND"
  ],
  "responseTimeout": "1s",
  "exceptionErrorResponses": [
    {
      "name": "Resource_Exhausted",
      "action": "Send_Answer",
      "error_code": 503,
      "error_response": "Service Unavailable"
    },
    {
      "name": "No_Response",
      "action": "Send_Answer",
      "error_code": 503,
      "error_response": "Service Unavailable"
    },
    {
      "name": "Connect_Failure",
      "action": "Send_Answer",
      "error_code": 503,
      "error_response": "Service Unavailable"
    },
    {
      "name": "No_Host",
      "action": "Send_Answer",
      "error_code": 503,
```

```
      "error_response": "Service Unavailable"
    },
    {
      "name": "Db_LookUp_Error",
      "action": "Send_Answer",
      "error_code": 500,
      "error_response": "Session/Subscriber binding not found/look-up
failure at OCSCP-SDS Service"
    }
  ],
  "deploymentModel": "SITE_WIDE",
  "name": "nudm-uecm"
}
```

Request_Type: PUT

URL: */soothsayer/v1/routingoptions/*

Port: 8081

Message

```
curl -X PUT http://<Soothsayerfqdn>:8081/soothsayer/v1/routingoptions/
namf-comm/ \
-H 'Content-Type: application/json' \
-d '{
  "pod": {
    "maxPendingResponses": 1000,
    "maxRoutingAttempts": 2,
    "alternateRouting": true,
    "loadBalancingAlgorithm": "Round_Robin"
  },
  "srv": {
    "name": "namf-comm",
    "maxPendingResponses": 1000,
    "maxRoutingAttempts": 3,
    "actions": "Forward",
    "loadBalancingAlgorithm": "Priority_only",
    "nfServiceLoadBasedCongestionControl": {
      "alternateRoutingOnsetThresholdPercent": 80,
      "alternateRoutingAbatementThresholdPercent": 75,
      "throttleOnsetThresholdPercent": 90,
      "throttleAbatementThresholdPercent": 85,
      "responseErrorCode": 503
    },
    "defaultPriority": 1,
    "defaultCapacity": 65535,
    "reverseProxySupport": true,
    "initialServiceRequest": {
      "routePolicy": "Forward_Route",
      "reroutePolicy": "RerouteWithinSite"
    },
    "subsequentServiceRequest": {
      "routePolicy": "Forward_Route",
      "reroutePolicy": "RerouteWithinSite"
```

```
    }
  },
  "totalTransactionLifetime": "6s",
  "reRouteOnResponseCodeList": [
    "ALL_SERVER_ERROR",
    "NOT_FOUND",
    "REQUEST_TIMEOUT",
    "RETRIABLE_4XX",
    "GONE",
    "TOO_MANY_REQUESTS",
    "TEMPORARY_REDIRECT",
    "PERMANENT_REDIRECT"
  ],
  "responseTimeout": "1s",
  "exceptionErrorResponses": [
    {
      "name": "Resource_Exhausted",
      "action": "Send_Answer",
      "error_code": 503,
      "error_response": "Service Unavailable"
    },
    {
      "name": "No_Response",
      "action": "Send_Answer",
      "error_code": 503,
      "error_response": "Service Unavailable"
    },
    {
      "name": "Connect_Failure",
      "action": "Send_Answer",
      "error_code": 503,
      "error_response": "Service Unavailable"
    },
    {
      "name": "No_Host",
      "action": "Send_Answer",
      "error_code": 503,
      "error_response": "Service Unavailable"
    },
    {
      "name": "Db_LookUp_Error",
      "action": "Send_Answer",
      "error_code": 500,
      "error_response": "Session/Subscriber binding not found/look-up
failure at OCSCP-SDS Service"
    }
  ],
  "deploymentModel": "SITE_WIDE",
  "name": "namf-comm"
}'
```

Request_Type: PATCH

URL: */soothsayer/v1/routingoptions/*

Port: 8081

Message

```
curl -X PATCH http://<Soothsayerfqdn>:8081/soothsayer/v1/routingoptions/
<service name> \
            -H 'Content-Type: application/merge-patch+json' \
            -d '{
            "srv": {
                    "name": "nudm-uecm",
                    "reverseProxySupport": true
              },
              "exceptionErrorResponses": [
                {
                      "name": "Db_LookUp_Error",
                      "action": "Send_Answer",
                      "error_code": 500,
                      "error_response": "Session/Subscriber binding not
found/look-up failure at OCSCP-SDS Service"
                    }
              ]
        }
    }'
```

Configuring Mediation Options

Mediation service supports 5G HTTP2 message manipulation techniques. SCP allows routing of messages to mediation service based on specific parameters. These parameters may include NfType, NfService, MessageType, any standard HTTP2 header and/or Information Elements from JSON payload.

Configuration parameters

Table 3-6 Mediation Configuration

Filed Name	Type	Description
nfType	enum NFType	NFType for which mediation configuration is to be done
nfService	String	Service of NFType for which mediation configuration is to be done
messageType	String	Message of Service for which mediation configuration is to be done
match	Match	List of match blocks to be satisfied for the rule to be activated. The list of match blocks have OR semantics. Minimum number of blocks = 1 Maximum number of blocks = 20
groupId	String	groupId for which mediation configuration is to be done. Mediation configuration for a specific group shall be applicable to the mediation requests/ responses received from the same group only. HTTP Mediation service consumer NFs which requires same mediation rules can be grouped together using this groupId.

Table 3-6 (Cont.) Mediation Configuration

Filed Name	Type	Description
Trigger Points	triggerPoints	List of trigger points to be enabled if matches. One or more of following: `"requestIngress", "requestEgress", "responseIngress", "responseEgress"`

Match

Table 3-7 Match

Field	Data Type	Description	Required
name	String	Unique name for the match block within this configuration.	Yes
headers	HeaderBodyMatch[]	List of header name and header value to match using MatchType comparison. All conditions inside a single header block have AND semantics. Minimum number of elements/conditions = 1 Maximum number of elements/conditions = 5	anyOf (either or both)
body	HeaderBodyMatch[]	List of "body IE" JSON Pointer and value at that Pointer to match using MatchType comparison. All conditions inside a single body block have AND semantics. Minimum number of elements/conditions = 1 Maximum number of elements/condition = 5	anyOf (either or both)

HeaderBodyMatch

Table 3-8 HeaderBodyMatch

Field	Data Type	Description	Required
name	String	Name of the header or the bodyIE JSON Pointer. **Notes**:List of predefined headers available at in this section. JSON Pointer must point to basic data types. Arrayed and Object values are not supported.	Yes
match_type	MatchType	One of the supported match operator.	Yes
value	String	Value of header or bodyIE to be matched. value is only required if match_type is not *range*.	Conditional
start	Integer	Range start (inclusive). Only used when match_type is *range*.	Conditional
end	Integer	Range end (inclusive). Only used when match_type is *range*.	Conditional

MatchType

Table 3-9 MatchType

Field	Data Type	Description	Required
exact	String	Matching is performed using exact comparison	oneOf
prefix	String	Matching is performed using prefix comparison	oneOf
regex	String	Matching is performed using ECMAScript Regular Expression comparison	oneOf
range	String	Matching is performed using range comparison	oneOf

Configuring Operations for Mediation Options

User can configure routing options by using the operations GET, PUT, PATCH and DELETE.

The following sections provide sample details of the operations to configure mediation options.

Request_Type: GET

URL: /soothsayer/v1/mediationconfiguration/

Message

```
[
  {
    "nfType": "AUSF",
    "nfService": "nausf-auth",
    "messageType": "ue-authentications",
    "match": [
      {
        "name": "invalid-suci",
        "body": [
          {
            "name": "/supiOrSuci",
            "value": ".*0-0-0.*",
            "match-type": "regex"
          }
        ]
      }
    ],
    "triggerPoints": [
      "requestIngress"
    ],
    "groupId": "scp",
    "id": "ausf@nausf-auth@ue-authentications"
  }
]
```

Request_Type: PUT

URL: /soothsayer/v1/mediationconfiguration/

Message

```
'{
    "nfType":"AUSF",
    "nfService":"nausf-auth",
    "messageType":"ue-authentications",
    "match":[
        {"name":"invalid-suci",
        "body":[
            {"name":"/supiOrSuci",
            "value":".*0-0-0.*",
            "match-type":"regex"}]}],
```

```
    "triggerPoints":["requestIngress"],"groupId":"scp"
    }'
```

Request_Type: PATCH

URL: /soothsayer/v1/mediationconfiguration/

Message

```
'{
    "triggerPoints":["requestIngress", "responseEgress"],
    "groupId":"scp"
    }'
```

Request_Type: DELETE

URL: /soothsayer/v1/mediationconfiguration/

Message

```
curl -X DELETE "http://10.178.254.214:32655/soothsayer/v1/
mediationconfiguration/NRF?serviceName=nnrf-disc" -H  "accept: text/
plain"
```

Configuring MessagePriority Options

Message Priority assignment/override is supported for below 5G NFs. User can configure routing options by using the operations **LIST**, **GET**, **PUT** and **PATCH**.

- NRF
  Message Priority assignment/override is supported for below NF services:
  - Nnrf_NFManagement Service
    - All message supported except Notification Callback messages.
  - Nnrf_NFDiscovery Service
- UDM
  Message Priority assignment/override is supported for below NF services:
  - Nudm_SubscriberDataManagement Service
  - Nudm_UEContextManagement Service
  - Nudm_UEAuthentication Service
  - Nudm_EventExposure Service
  - Nudm_ParameterProvision Service
- PCF
  Message Priority assignment/override is supported for below NF services:
  - Npcf_AMPolicyControl Service
  - Npcf_SMPolicyControl Service
  - Npcf_PolicyAuthorization Service

  - Npcf_BDTPolicyControl Service
- CHF
  Message Priority assignment/override is supported for below NF services:
  - Nchf_SpendingLimitControl
  - Nchf_ConvergedCharging
- AUSF
  Message Priority assignment/override is supported for below NF services:
  - Nausf_UEAuthentication

"3gpp-Sbi-Message-Priority" header carries the message priority of 5G messages. The SCP includes/modifies the header based on the configuration parameters.

HTTP2 stream priorities are valid only per connection, it is not an E2E mechanism so to have it:

- 3gpp-Sbi-Message-Priority header contains the HTTP/2 message priority value anything between 1 to 256. The default is 16.

Table 3-10 Configuring Parameters for MessagePriority Options

Operation	Parameter	Type	Description	REST Command

LIST	-	-	-	curl --header 'Content-type: application/json' --header 'accept: application/json' --request GET 'http://<Soothsayerfqdn>:8081/soothsayer/v1/messagepriority'
				[
				{
				"requestResponse": "REQUEST",
				"nfServiceName": "nudm-uecm",
				"messageType": "amf-3gpp-access",
				"whenHeaderPresent": {
				"overrideFlag": false,
				"headerValue": ""
				},
				"whenHeaderNotPresent": {
				"overrideFlag": false,
				"headerValue": ""
				}
				},
				{
				"requestResponse": "RESPONSE",
				"nfServiceName": "nudm-uecm",
				"messageType": "amf-3gpp-access",
				"whenHeaderPresent": {
				"overrideFlag": false,
				"headerValue": ""
				},
				"whenHeaderNotPresent": {
				"overrideFlag": true,
				"headerValue": ""
				}
				},

Table 3-10 (Cont.) Configuring Parameters for MessagePriority Options

Operation	Parameter	Type	Description	REST Command
				...]

Table 3-10 (Cont.) Configuring Parameters for MessagePriority Options

Operation	Parameter	Type	Description	REST Command

GET	-	-	-	curl --header 'Content-type: application/json' --header 'accept: application/json' --request GET 'http://<Soothsayerfqdn>:8081/soothsayer/v1/messagepriority?nfServiceName=<serviceName>&messageType=amf-3gpp-access'
				[
				{
				"requestResponse": "REQUEST",
				"nfServiceName": "nudm-uecm",
				"messageType": "amf-3gpp-access",
				"whenHeaderPresent": {
				"overrideFlag": false,
				"headerValue": ""
				},
				"whenHeaderNotPresent": {
				"overrideFlag": false,
				"headerValue": ""
				}
				},
				{
				"requestResponse": "RESPONSE",
				"nfServiceName": "nudm-uecm",
				"messageType": "amf-3gpp-access",
				"whenHeaderPresent": {
				"overrideFlag": false,
				"headerValue": ""
				},
				"whenHeaderNotPresent": {
				"overrideFlag": true,

Table 3-10 (Cont.) Configuring Parameters for MessagePriority Options

Operation	Parameter	Type	Description	REST Command

				<pre>"headerValue": ""
				}
				}
				]</pre>

PUT	requestResponse	Enum	• If the value is RESPONSE - Egress Response
			• If the value is REQUEST - Ingress Request
				Set the value of field requestResponse and masterIP and Configuration as REQUEST or RESPONSE in the curl command below **requestResponse UPDATE Command**
				
				<pre>curl -X PUT \
				http://
				<Soothsayerfqdn>:8081/
				soothsayer/v1/
				messagepriority \
				-H 'Content-Type:
				application/json' \
				-d '{
				"requestResponse" :
				"REQUEST",
				"nfServiceName" :
				"nudm-uecm",
				"messageType" :
				"amf-3gpp-access",
				"whenHeaderPresent" : {
				"overrideFlag" : false,
				"headerValue" : "10"
				},
				"whenHeaderNotPresent" :
				{
				"overrideFlag" : true,
				"headerValue" : "5"
				}
				}'</pre>

Table 3-10 (Cont.) Configuring Parameters for MessagePriority Options

Operation	Parameter	Type	Description	REST Command

	nfServiceName	String	Name of the NF Service
			List of NF Services
			
			nnrf-disc
			nnrf-nfm
			nnwdaf-analyticsinfo
			nsmsf-sms
			nnwdaf-eventssubscription
			nudr-dr
			nlmf-loc
			nchf-spendinglimitcontrol
			nchf_convergedcharging
			nbsf-management
			nnssf-nssaiavailability
			n5g-eir-eic
			nnssf-nsselection
			nudm-ee
			nudm-ueau
			nudm-sdm
			nudm-uecm
			nudm-pp
			nnef-pfdmanagement
			namf-com
			namf-evts
			namf-mt
			namf-location
			nausf-sorprotection
			nsmf-event-exposure
			nsmf-pdusession
			nausf-auth
			nausf_ueauthentication
			npcf-smpolicycontrol
			npcf-am-policy-control
			npcf-bdtpolicycontrol
			npcf-policyauthorization
				Set the value of field nfServiceName in the curl command below **nfServiceName UPDATE Command**
				
				curl -X PUT \
				http://<Soothsayerfqdn>:8081/soothsayer/v1/messagepriority \
				-H 'Content-Type: application/json' \
				-d '{
				"requestResponse" : "REQUEST",
				"nfServiceName" : "nudm-uecm",
				"messageType" : "amf-3gpp-access",
				"whenHeaderPresent" : {
				"overrideFlag" : false,
				"headerValue" : "10"
				},
				"whenHeaderNotPresent" : {
				"overrideFlag" : true,
				"headerValue" : "5"
				}
				}'

Table 3-10 (Cont.) Configuring Parameters for MessagePriority Options

Operation	Parameter	Type	Description	REST Command

	messageType	String	Message type for given service name MessageType List	Set the value of field messageType for the mentioned NF Service in the curl command below **messageType UPDATE Command**
				
				`curl -X PUT \`
				` http://`
				`<Soothsayerfqdn>:8081/`
				`soothsayer/v1/`
				`messagepriority \`
				` -H 'Content-Type:`
				`application/json' \`
				` -d '{`
				` "requestResponse" :`
				`"REQUEST",`
				` "nfServiceName" :`
				`"nudm-uecm",`
				` "messageType" :`
				`"amf-3gpp-access",`
				` "whenHeaderPresent" : {`
				`  "overrideFlag" : false,`
				`  "headerValue" : "10"`
				` },`
				` "whenHeaderNotPresent" :`
				`{`
				`  "overrideFlag" : true,`
				`  "headerValue" : "5"`
				` }`
				`}'`

Table 3-10 (Cont.) Configuring Parameters for MessagePriority Options

Operation	Parameter	Type	Description	REST Command

	whenHeaderPresent.overrideFlag	boolean	Override Flag for the case when Header is Present	Set the value of field overrideFlag section in the curl command below
				overrideFlag UPDATE Command
				
				`curl -X PUT \`
				` http://`
				`<Soothsayerfqdn>:8081/`
				`soothsayer/v1/`
				`messagepriority \`
				` -H 'Content-Type:`
				`application/json' \`
				` -d '{`
				` "requestResponse" :`
				`"REQUEST",`
				` "nfServiceName" :`
				`"nudm-uecm",`
				` "messageType" :`
				`"amf-3gpp-access",`
				` "whenHeaderPresent" : {`
				`  "overrideFlag" : false,`
				`  "headerValue" : "10"`
				` },`
				` "whenHeaderNotPresent" :`
				`{`
				`  "overrideFlag" : true,`
				`  "headerValue" : "5"`
				` }`
				`}'`

Table 3-10 (Cont.) Configuring Parameters for MessagePriority Options

Operation	Parameter	Type	Description	REST Command

	whenHeaderPresent.headerValue	String	Value of the priority header for the corresponding flag for the case when Header is Present	Set the value of field headerValue section in the curl command below **headerValue UPDATE Command**
				
				`curl -X PUT \`
				` http://`
				`<Soothsayerfqdn>:8081/`
				`soothsayer/v1/`
				`messagepriority \`
				` -H 'Content-Type:`
				`application/json' \`
				` -d '{`
				` "requestResponse" :`
				`"REQUEST",`
				` "nfServiceName" :`
				`"nudm-uecm",`
				` "messageType" :`
				`"amf-3gpp-access",`
				` "whenHeaderPresent" : {`
				`  "overrideFlag" : false,`
				`  "headerValue" : "10"`
				` },`
				` "whenHeaderNotPresent" :`
				`{`
				`  "overrideFlag" : true,`
				`  "headerValue" : "5"`
				` }`
				`}'`

Table 3-10 (Cont.) Configuring Parameters for MessagePriority Options

Operation	Parameter	Type	Description	REST Command

	whenHeaderNotPresent.overrideFlag	boolean	Override Flag for the case for the case when Header is not Present	Set the value of field overrideFlag section in the curl command below
				overrideFlag UPDATE Command
				
				`curl -X PUT \`
				` http://`
				`<Soothsayerfqdn>:8081/`
				`soothsayer/v1/`
				`messagepriority \`
				` -H 'Content-Type:`
				`application/json' \`
				` -d '{`
				` "requestResponse" :`
				`"REQUEST",`
				` "nfServiceName" :`
				`"nudm-uecm",`
				` "messageType" :`
				`"amf-3gpp-access",`
				` "whenHeaderPresent" : {`
				`  "overrideFlag" : false,`
				`  "headerValue" : "10"`
				` },`
				` "whenHeaderNotPresent" :`
				`{`
				`  "overrideFlag" : true,`
				`  "headerValue" : "5"`
				` }`
				`}'`

Table 3-10 (Cont.) Configuring Parameters for MessagePriority Options

Operation	Parameter	Type	Description	REST Command

	whenHeaderNotPresent.headerValue	String	Value of the priority header for the corresponding flag for the case when Header is not Present	Set the value of field headerValue section in the curl command below **headerValue UPDATE Command**
				
				`curl -X PUT \`
				` http://`
				`<Soothsayerfqdn>:8081/`
				`soothsayer/v1/`
				`messagepriority \`
				` -H 'Content-Type:`
				`application/json' \`
				` -d '{`
				` "requestResponse" :`
				`"REQUEST",`
				` "nfServiceName" :`
				`"nudm-uecm",`
				` "messageType" :`
				`"amf-3gpp-access",`
				` "whenHeaderPresent" : {`
				`  "overrideFlag" : false,`
				`  "headerValue" : "10"`
				` },`
				` "whenHeaderNotPresent" :`
				`{`
				`  "overrideFlag" : true,`
				`  "headerValue" : "5"`
				` }`
				`}'`

Table 3-10 (Cont.) Configuring Parameters for MessagePriority Options

Operation	Parameter	Type	Description	REST Command

PATCH		String	Modify message priority options for a particular service and message type.	curl -X PATCH \
				
				http://<Soothsayerfqdn>:8081/soothsayer/v1/messagepriority \
				
				-H 'Content-Type: application/merge-patch+json' \
				
				-d '{
				
				"requestResponse" : "REQUEST",
				
				"nfServiceName" : "nudm-uecm",
				
				"messageType" : "amf-3gpp-access",
				
				"whenHeaderPresent" : {
				
				"overrideFlag":true,
				
				"headerValue":"5"
				
				}
				
				}

Configuring SystemOptions

These options are used to control system behavior per service-wide. The user can configure SystemOptions by using the operations **GET** and **PUT**.

> **Note:**
>
> Default systemOptions are provided during the installation of Service Communication Proxy through helm.

REST Message sample

Request_Type: **GET and PUT**

URL: `http://<Soothsayerfqdn>:8081/soothsayer/v1/systemoptions`

```
{
    "cbEnabled": false,
    "odEnabled": false,
    "trafficPolicy": {
        "connectionPool": {
            "http": {
                "http2MaxRequests": 1000,
                "idleTimeout": "3600s"
            },
            "tcp": {
                "connectTimeout": "250ms",
                "tcpKeepalive": {
                    "probes": 9,
                    "time": "180s",
                    "interval": "60s"
                }
            }
        },
        "outlierDetection": {
            "consecutiveErrors": 5,
            "interval": "10s",
            "baseEjectionTime": "30s",
            "maxEjectionPercent": 100
        }
    }
}
```

Table 3-11 provides SystemOptions for the GET and PUT operations.

Table 3-11 Configuring Parameters for SystemOptions

Operation	Parameter	Value	Description
GET	-	-	Get System Options
PUT	cbEnabled	Boolean	Provides information whether the Circuit-Breaking is enabled or not. Default is false
	odEnabled	Boolean	Provides information whether the Outlier-Detection is enabled or not. Default is false
	trafficPolicy.connectionPool.http.http2MaxRequests	Integer	Maximum number of requests to a backend. Default is 1024.

Table 3-11 (Cont.) Configuring Parameters for SystemOptions

Operation	Parameter	Value	Description
	trafficPolicy.connectionPool.http.idleTimeout	String	The idle timeout for upstream connection pool connections. The idle timeout is defined as the period in which there are no active requests. If not set, there is no idle timeout. When the idle timeout is reached the connection will be closed. Note that request based timeouts mean that HTTP/2 PINGs will not keep the connection alive. Default is 3600s.
	trafficPolicy.connectionPool.tcp.connectTimeout	String	TCP Connection timeout. Valid time units are ns, us (or µs), ms, s. For example: 300ms.
	trafficPolicy.connectionPool.tcp.tcpKeepalive	TcpKeepalive	Contains TcpKeepalive information. If set, enable TCP Keepalives to upstream peer. All the parameters of tcpkeepAlive are needed if this information is being configured.
	trafficPolicy.connectionPool.tcp.tcpKeepalive.probes	Integer	Maximum number of keepalive probes to send without response before deciding the connection is dead. For example: 9 Default is to use the OS level configuration (unless overridden, Linux defaults to 9.)
	trafficPolicy.connectionPool.tcp.tcpKeepalive.time	String	The time duration a connection needs to be idle before keep-alive probes start being sent. Valid time units are ns, us (or µs), ms, s. For example: 180s Default is to use the OS level configuration (unless overridden, Linux defaults to 7200s (i.e. 2 hours.)
	trafficPolicy.connectionPool.tcp.tcpKeepalive.interval	String	The time duration between keep-alive probes. Valid time units are ns, us (or µs), ms, s. For example: 60s Default is to use the OS level configuration (unless overridden, Linux defaults to 75s.)
	outlierDetection.consecutiveErrors	Integer	Number of errors before a host is ejected from the connection pool. Defaults to 5. When the upstream host is accessed over HTTP, a 502, 503 or 504 return code qualifies as an error. When the upstream host is accessed over an opaque TCP connection, connect timeouts and connection error/failure events qualify as an error.
	outlierDetection.interval	String	Time interval between ejection sweep analysis. format: 1h/1m/1s/1ms. Must be >=1ms. Default is 10s.

Table 3-11 (Cont.) Configuring Parameters for SystemOptions

Operation	Parameter	Value	Description
	outlierDetection.baseEjectionTime	String	Minimum ejection duration. A host will remain ejected for a period equal to the product of minimum ejection duration and the number of times the host has been ejected. This technique allows the system to automatically increase the ejection period for unhealthy upstream servers. format: 1h/1m/1s/1ms. Must be >=1ms. Default is 30s.
	outlierDetection.maxEjectionPercent	Integer	Maximum % of hosts in the load balancing pool for the upstream service that can be ejected. Defaults to 10%.

Configuring Circuit Breaking and Outlier Detection

Outlier detection in SCP tracks the status of each individual endpoint of the producer NFs/NF Services. Upstream producer endpoints that continually returns 5xx errors for service requests are ejected from the routing pool for a pre-defined period of time.

Outlier detection is a form of *passive* health checking of producer NFs. Outlier detection is per endpoint (of producer NF instance) and triggers when SCP receives consecutively 5xx error response and exceeds the configurable number of consecutive 5xx errors.

Circuit breaking is triggered on a per FQDN basis when its outstanding transactions exceeds a configurable value. When circuit breaking is activated, requests are alternate routed if possible or rejected.

Operator configuration:

- Enable/Disable the circuit breaking on a per NF or FQDN basis.
- Outstanding transactions threshold beyond which Circuit breaking shall be invoked on a per NF or FQDN basis.

Table 3-12 provides information about the configuring parameters for outlier detection.

> **Note:**
>
> Circuit Breaking and Outlier Detection are global or system wide options.

Table 3-12 Outlier Detection Parameters

Parameter	Value	Description	Example

cbEnabled	Boolean	This tells whether Circuit-Breaking is enabled or not. Default: False	Set the value of field **cbEnabled** in the curl command below:
			
			`curl -X PUT \`
			` http://<Soothsayerfqdn>:8081/soothsayer/v1/systemoptions \`
			` -H 'Content-Type: application/json' \`
			` -d '{`
			`  "cbEnabled": False,`
			`  "odEnabled": False,`
			`  "trafficPolicy": {`
			`  "connectionPool": {`
			`  "http": {`
			`  "http2MaxRequests": 1000`
			`  }`
			`  },`
			`  "outlierDetection": {`
			`  "consecutiveErrors": 5,`
			`  "interval": "10s",`
			`  "baseEjectionTime": "30s",`
			`  "maxEjectionPercent": 100`
			`  }`
			`  }`
			` }'`

Table 3-12 (Cont.) Outlier Detection Parameters

Parameter	Value	Description	Example

odEnabled	Boolean	This tells whether Outlier-Detection is enabled or not. Default: False	Set the value of field **odEnabled** in the curl command below:
			
			`curl -X PUT \`
			` http://<Soothsayerfqdn>:8081/soothsayer/v1/systemoptions \`
			` -H 'Content-Type: application/json' \`
			` -d '{`
			`  "cbEnabled": False,`
			`  "odEnabled": False,`
			`  "trafficPolicy": {`
			`  "connectionPool": {`
			`  "http": {`
			`  "http2MaxRequests": 1000`
			`  }`
			`  },`
			`  "outlierDetection": {`
			`  "consecutiveErrors": 5,`
			`  "interval": "10s",`
			`  "baseEjectionTime": "30s",`
			`  "maxEjectionPercent": 100`
			`  }`
			`  }`
			` }'`

Table 3-12 (Cont.) Outlier Detection Parameters

Parameter	Value	Description	Example

trafficPolicy.connectionPool.http.http2MaxRequests	Integer	Maximum number of requests to a backend. Default 1024.	Set the value of field **http2MaxRequests** under **trafficPolicy.connectionPool.http** in the curl command below:
			
			`curl -X PUT \`
			`http://<Soothsayerfqdn>:8081/soothsayer/v1/systemoptions \`
			`-H 'Content-Type: application/json' \`
			`-d '{`
			`"cb_and_od_enabled": true,`
			`"trafficPolicy": {`
			`"connectionPool": {`
			`"http": {`
			`"http2MaxRequests": 1000`
			`}`
			`},`
			`"outlierDetection": {`
			`"consecutiveErrors": 5,`
			`"interval": "10s",`
			`"baseEjectionTime": "30s",`
			`"maxEjectionPercent": 100`
			`}`
			`}`
			`}'`

Table 3-12 (Cont.) Outlier Detection Parameters

Parameter	Value	Description	Example

outlierDetection.consecutiveErrors	Integer	5G defined NF Type. For example, BSF, UDR, UDSF, etc.	Set the value of **ConsecutiveErrors** field under outlierDetection in the curl command below **consecutiveErrors UPDATE Command**
			
			`curl -X PUT \`
			` http://<Soothsayerfqdn>:8081/soothsayer/v1/systemoptions \`
			` -H 'Content-Type: application/json' \`
			` -d '{`
			`  "cb_and_od_enabled": true,`
			`  "trafficPolicy": {`
			`  "connectionPool": {`
			`  "http": {`
			`  "http2MaxRequests": 1000`
			`  }`
			`  },`
			`  "outlierDetection": {`
			`  "consecutiveErrors": 5,`
			`  "interval": "10s",`
			`  "baseEjectionTime": "30s",`
			`  "maxEjectionPercent": 100`
			`  }`
			`  }`
			` }'`

Table 3-12 (Cont.) Outlier Detection Parameters

Parameter	Value	Description	Example

outlierDetection.interval	String	Time interval between ejection sweep analysis.
		Format: 1h/1m/1s/1ms.
		MUST BE >=1ms.
		Default is 10s
			Set the value of **interval** field under outlierDetection in the curl command below
			interval UPDATE Command
			
			`curl -X PUT \`
			` http://<Soothsayerfqdn>:8081/soothsayer/v1/systemoptions \`
			` -H 'Content-Type: application/json' \`
			` -d '{`
			`  "cb_and_od_enabled": true,`
			`  "trafficPolicy": {`
			`  "connectionPool": {`
			`  "http": {`
			`  "http2MaxRequests": 1000`
			`  }`
			`  },`
			`  "outlierDetection": {`
			`  "consecutiveErrors": 5,`
			`  "interval": "10s",`
			`  "baseEjectionTime": "30s",`
			`  "maxEjectionPercent": 100`
			`  }`
			`  }`
			` }'`

Table 3-12 (Cont.) Outlier Detection Parameters

Parameter	Value	Description	Example

outlierDetection.baseEjectionTime	String	Minimum ejection duration.
		Format: 1h/1m/1s/1ms.
		MUST BE >=1ms.
		Default is 30s.
			Set the value of field baseEjectionTime under outlierDetection in the curl command below
			baseEjectionTime UPDATE Command
			
			`curl -X PUT \`
			`http://<Soothsayerfqdn>:8081/soothsayer/v1/systemoptions \`
			`-H 'Content-Type: application/json' \`
			`-d '{`
			`"cb_and_od_enabled": true,`
			`"trafficPolicy": {`
			`"connectionPool": {`
			`"http": {`
			`"http2MaxRequests": 1000`
			`}`
			`},`
			`"outlierDetection": {`
			`"consecutiveErrors": 5,`
			`"interval": "10s",`
			`"baseEjectionTime": "30s",`
			`"maxEjectionPercent": 100`
			`}`
			`}`
			`}'`

Table 3-12 (Cont.) Outlier Detection Parameters

Parameter	Value	Description	Example
outlierDetection.maxEjectionPercent	Integer	Maximum percentage of hosts in the load balancing pool for the upstream service that can be ejected.	Set the value of field maxEjectionPercent under outlierDetection in the curl command below **maxEjectionPercent UPDATE Command** `curl -X PUT \ http://<Soothsayerfqdn>:8081/soothsayer/v1/systemoptions \ -H 'Content-Type: application/json' \ -d '{ "cb_and_od_enabled": true, "trafficPolicy": { "connectionPool": { "http": { "http2MaxRequests": 1000 } }, "outlierDetection": { "consecutiveErrors": 5, "interval": "10s", "baseEjectionTime": "30s", "maxEjectionPercent": 100 } } }'`

Configuring NF Service Groups

SCP provides NF/Service Group Configuration, where the operator provides the primary and secondary CHF instance information to create the routing rules based

on the CHF NF topology information provided by the NRF via NF register/reregister/change notifications.

Parameters for Configuring NF Service Groups

Table 3-13 Parameters for NF Service Groups

Resource Name	Resource URI	HTTP method or custom operation	Description
servicegroups	{apiRoot}/soothsayer/v1/servicegroups/{serviceName} Ex: {apiRoot}/soothsayer/v1/servicegroups/nchf-spendinglimitcontrol	GET	Returns the NF Service for a given serviceName.
servicegroups	{apiRoot}/soothsayer/v1/servicegroups?nfType=value Ex: {apiRoot}/soothsayer/v1/servicegroups?nfType=CHF	GET	Returns a list of NF Services for a given NF Type.
servicegroups	{apiRoot}/soothsayer/v1/servicegroups	PUT	Updates the NF Service.
servicegroups	{apiRoot}/soothsayer/v1/servicegroups?nfType=value&serviceName=value Ex: {apiRoot}/soothsayer/v1/servicegroups?nfType=CHF&serviceName=nchf-spendinglimitcontrol	PATCH	Updates a single NF Service based on serviceName or Updates multiple NF Services based on NF Type.
servicegroups	{apiRoot}/soothsayer/v1/servicegroups/{serviceName} Ex: {apiRoot}/soothsayer/v1/servicegroups/nchf-spendinglimitcontrol	DELETE	Deletes the given NFService with serviceName.
servicegroups	{apiRoot}/soothsayer/v1/servicegroups?nfType=value Ex: {apiRoot}/soothsayer/v1/servicegroups?nfType=CHF	DELETE	Deletes all the services for a given NF Type.

Resource Definition

Table 3-14 Supported Parameters

Query Parameter	Request Body	HTTP method or custom operation	Data type	P	Cardinality	Response Codes	Description
servicename	n/a	GET	NFServiceGroup	M	1	200 OK	Upon success, a response body is returned containing the NFServiceGroup for requested Service Name.
			String	M	1	404 NOT FOUND	The response body contains the message indicating that the there were no services found for the requested Service Name.
serviceName: Optional nfType: Optional **Note**: Either one of above parameters are mandatory. Both cannot be left empty.	NFServiceGroupModifiableFields object with any of the attributes. Note: Data Model for this request body is provided in "Data Models" section.	PATCH	String	M	1	200 OK	Upon success, following message is returned: Updated NF Service with serviceName: nchf-spendinglimitcontrol

Table 3-14 (Cont.) Supported Parameters

Query Parameter	Request Body	HTTP method or custom operation	Data type	P	Cardinality	Response Codes	Description
			String	M	1	403 FORBIDDEN	primaryRegionLocalities can not be empty or its size cannot be zero.
			String	M	1	400 BAD REQUEST	If both request parameters are missing then Bad Request error would be returned with following message: Please pass either serviceName or nfType.
serviceName	n/a	DELETE	String	M	1	200 OK	Upon success, following message is returned: Successfully deleted the Nf Service for ServiceName: `nchf-spendinglimitcontrol`

Table 3-14 (Cont.) Supported Parameters

Query Parameter	Request Body	HTTP method or custom operation	Data type	P	Cardinality	Response Codes	Description
nfType	n/a	GET	List<NFServiceGroup>	M	1	200 OK	Upon success, a response body is returned containing a List of NFServiceGroup's for requested nfType.
			String	M	1	404 BAD REQUEST	Required parameter 'nfType' is not present.
		DELETE	String	M	1	200 OK	Upon success, following message is returned: Successfully deleted all Services for NFType : CHF.
n/a	"NFServiceGroup" object with updated fields. Note: Sample data is provided in Example column and also the "Data Model" for this Request Body	PUT	NFServiceGroup	M	1	200 OK	Upon success, a response body is returned containing the updated NFServiceGroup object.

Table 3-14 (Cont.) Supported Parameters

Query Parameter	Request Body	HTTP method or custom operation	Data type	P	Cardinality	Response Codes	Description
	could be found in the "Data Models" section.		String	M	1	403 FORBIDDEN	Not allowed to modify NfType or serviceName of NFServiceGroup.
			String	M	1	400 BAD REQUEST	If any of the mandatory parameters are missing in the Request Body, then BAD REQUEST error would be returned. Note: Refer to Data Model for Mandatory parameters.

Table 3-14 (Cont.) Supported Parameters

Query Parameter	Request Body	HTTP method or custom operation	Data type	P	Cardinality	Response Codes	Description
			String	M	1	400 BAD REQUEST	If "primaryRegionLocalities" attribute in Request Body is assigned with empty list, then a BAD REQUEST error would be returned as this value cannot be empty. Response message: Primary Region Localities for a NF Service cannot be Null or empty.

Data Models for NF Service Groups

NFServiceGroup

Table 3-15 NFServiceGroup

Field Name	Type	P	Description(With default Values)
nfType	Enum	M	NRF, UDM, AMF, SMF, AUSF, NEF, PCF, SMSF, NSSF, UDR, LMF, GMLC, 5GEIR, SEPP, UPF, N3IWF, AF, UDSF, BSF, CHF, NWDAF, CUSTOM_ORACLE_SCP Note: This parameter cannot be modified.
serviceName	String	M	Only CHF Services are supported currently: nchf-convergedcharging, nchf-spendinglimitcontrol Note: This parameter cannot be modified.

Table 3-15 (Cont.) NFServiceGroup

Field Name	Type	P	Description(With default Values)
primaryRegionLocalities	List<String>	M	This parameter can be modified but, empty values cannot be assigned to this parameter.
secondaryRegionLocalities	List<String>	O	This is an optional parameter and can also be modified.

ReroutePolicy

Table 3-16 ReroutePolicy

Field Name	Type	P	Description(With default Values)
rerouteOptions	Enum	M	Possible values: RerouteDisabled, RerouteWithinRegion, RerouteAcrossRegion

NFServiceGroupModifiableFields

Table 3-17 NFServiceGroupModifiableFields

Field Name	Type	P	Description(With default Values)
primaryRegionLocalities	List<String>	O	This parameter can be modified but, empty values cannot be assigned to this parameter.
secondaryRegionLocalities	List<String>	O	

Configuring Operations for NF Service Groups

User can configure routing options by using the operations GET, PUT and PATCH.

The following table provides sample details of the operations to configure routing options.

Table 3-18 NF Service Groups Operations

GET	`curl -X GET "http://10.178.246.62:31108/soothsayer/v1/servicegroups/nchf-spendinglimitcontrol" -H "accept: application/json"`

Table 3-18 (Cont.) NF Service Groups Operations

PUT	`curl -X PUT "http://10.178.246.62:31108/soothsayer/v1/servicegroups"`
	
	`-H "accept: application/json"`
	
	`-H "Content-Type: application/json"`
	
	`-d "{ \"nfType\": \"CHF\", \"serviceName\": \"nchf-spendinglimitcontrol\", \"primaryRegionLocalities\": [ \"Loc7\", \"USEast\",\"Loc6\" ], \"secondaryRegionLocalities\": [ \"Loc8\", \"Loc9\" ], \"reroutePolicy\": { \"rerouteOptions\": \"RerouteWithinRegion\" } } }"`

PATCH	`curl -X PATCH "http://10.178.246.62:31108/soothsayer/v1/servicegroups?serviceName=nchf-spendinglimitcontrol"`
	
	`-H "accept: application/json"`
	
	`-H "Content-Type: application/merge-patch+json"`
	
	`-d "{ \"primaryRegionLocalities\": [ \"Loc7\" ] }"`

Configuring NF Topology Groups

This section describes the configuration at SCP, which allows SCP to learn the 5G topology from NRF and use it for creating the routing rules or stop learning the 5G topology info NRF and use the user configured/updated NF profiles (SCP will not delete any already learned 5G topology info from NRF, when it stops learning from NRF).

5G Topology source info

This is the configuration which will be used by SCP to determine the 5G topology source and SCP will learn and create the routing rules accordingly.
TopologySourceInfo

Table 3-19 TopologySourceInfo

NF Type (M)	5G topology source (M)
• All 3gpp 5G defined NF types – As defined in TS29.510 section 6.1.6.3.3 String: NFType • Custom NF types	• NRF (default) – learning from NRF • LOCAL

Enumeration: TopologySource

Table 3-20 Enumeration: TopologySource

Enumeration value	Description
"NRF"	SCP 5G Topology info source is NRF.
"LOCAL"	SCP 5G Topology info source is user configured and not from NRF. This status may result from a NF Service failure and may trigger restoration procedures (see clause 6.2 of 3GPP 23.527 [27]). • transition from NRF ==> LOCAL: stop learning from NRF and use available/ modified/created info at SCP from now onwards. • transition from LOCAL ==> NRF: start learning from NRF and create the routing rules accordingly. In this scenario statically configured NF rules may get deleted (as there info is not available at NRF).

Table 3-21 Resources and Methods Overview

Resource name	Resource URI	HTTP method or custom operation	Request Body, Query Parameters	Response Status code, Body	Description
topologysource	{apiroot}/soothsayer/v1/topologysource	PUT	Body • Topology Source	200 OK	Create/update the topology source info for all the NF types.
		GET	Query Parameters • NFType		Read the topology source info for all the NF types.
NFtopologysource (individual NF types)	{apiroot}/soothsayer/v1/topologysource/{NFType}	PUT	Body • Topology Source	200 OK	Create/update the topology source info for a specific NF type.

Table 3-21 (Cont.) Resources and Methods Overview

Resource name	Resource URI	HTTP method or custom operation	Request Body, Query Parameters	Response Status code, Body	Description
		GET	Query Parameters • NFType		Read the topology source info for a specific NF type.

5G NF topology Info

This is the information for configuring 5G NF Profiles for NF for which source has been set as 'Local'. User can modify the 5G NF Profile irrespective of whether they are learnt from NRF (i.e. source='NRF) or configured statically (i.e source='Local') once learning source is set to 'Local'. Setting source to Local will not delete already learnt profiles.

Table 3-22 Parameters for NF Topology Groups

Resource name	Resources and Methods Overview	HTTP method or custom operation	Request Body, Query Parameters	Response Status code, Body	Description
nf-instances (Store)	{apiRoot}/soothsayer/v1/nf-instances/	GET	Query Parameters • NFType • ServiceName • NF instance Id • Max number of NF profiles • Max payload size see below Query parameters section.	• 200, OK, SearchResult, See below SearchResult section. • 400 Bad Request, ProblemDetails • 500 Internal server error, ProblemDetails	Read a collection of NF Instances.

Table 3-22 (Cont.) Parameters for NF Topology Groups

Resource name	Resources and Methods Overview	HTTP method or custom operation	Request Body, Query Parameters	Response Status code, Body	Description
	{apiRoot}/soothsayer/v1/nf-instances/nfInstanceIds	GET	Query Parameters • NFType (M) • array(ServiceName) (O)	• 200, OK, UriList, See below urList section. – The response body contains a "_links" object containing the URI of each NF in the SCP, or an empty object if there are no NFs to return in the query result (e.g., because there are no learned/configured NFs in the SCP, or because there are no matching NFs of the type specified in the "nf-type" query parameter). • 400 Bad Request, ProblemDetails • 500 Internal server error, ProblemDetails	Read a collection of NF Instance Id.
nf-instance (Document)	{apiRoot}/soothsyaer/v1/nf-instances/{nfInstanceID}	GET	Query Parameters • n/a Body • n/a	200 OK, NFProfile	Read the profile of a given NF Instance.
		PUT	Body • NFProfile	200 OK, NFProfile 201 Created, NFProfile	Register/ configure in SCP a new NF Instance, or replace the profile of an existing NF Instance, by providing an NF profile.

Table 3-22 (Cont.) Parameters for NF Topology Groups

Resource name	Resources and Methods Overview	HTTP method or custom operation	Request Body, Query Parameters	Response Status code, Body	Description
		PATCH	Body • PatchDocument – It contains the list of changes to be made to the profile of the NF Instance, according to the JSON PATCH format specified in IETF RFC 6902.	• 200 OK, NFProfile • 204, NO content	Modify the NF profile of an existing NF Instance.
		DELETE	Query • n/a Body • n/a	• 204, NO content	Deregister/ delete from SCP a given NF Instance.

Query Parameters

Table 3-23 Query Parameters

Name	Data Type	P	Cardinality	Description	Applicability
nf-type	NFType	M	1	This IE shall contain the NF type of the NF Service Producer being queried.	NF type of the NF Instances whose status is requested to be monitored.

Table 3-23 (Cont.) Query Parameters

Name	Data Type	P	Cardinality	Description	Applicability
service-names	array(ServiceName)	O	1..N	If included, this IE contains an array of service names for which the SCP is queried to provide the list of NF profiles. The SCP returns the NF profiles that have at least one NF service matching the NF service names in this list. If not included, the NRF returns all the NF service names registered in the NF profile.	Service name offered by the NF Instances whose status is requested to be monitored. This parameter is optional but if provided it returns with NF profile information.
nf-instance-id	NfInstanceId	O	0..1	Identity of the NF instance being queried.	NF Instance ID of the NF Instance whose status is requested to be monitored.
limit	integer	O	0..1	Maximum number of NFProfiles to be returned in the response.	Query-Params-Ext1
max-payload-size	integer	O	0..1	Maximum payload size (before compression, if any) of the response, expressed in kilo octets. When present, the NRF limits the number of NF profiles returned in the response such as to not exceed the maximum payload size indicated in the request. Default = 124. Maximum = 2000 (i.e. 2 Mo).	Query-Params-Ext1

SearchResult

Table 3-24 SearchResult

Attribute name	Data type	P	Cardinality	Description
nfInstances	array(NFProfile)	M	1..N	It contains an array of NF Instance profiles, matching the search criteria indicated by the query parameters of the query request. An empty array means there is no NF instance that can match the search criteria.

uriList

Table 3-25 uriList

Attribute name	Data type	P	Cardinality	Description
_links	map(LinksValueSchema)	O	1..N	See clause 4.9.4 of 3GPP TS 29.501 for the description of the members

Configuring NFProfile

Following are the minimum information required by SCP for statically configuring NFProfile.

Note: All the below mentioned parameters are according to spec 3GPP TS 29.510 and any parameters other than below mentioned are not used in SCP.

Table 3-26 Configuring NFProfile

Attribute name	Data type	P	Cardinality	Description
nfInstanceId	String	M	1	Identity of the NF instance being queried.
nfType	NFType	M	1	This IE contains the NF type of the NF Service Producer being queried.
nfStatus	NFStatus	M	1	This contains the NF status of NF Service Producer.
nsiList	array(String)	O	0..N	Only returned in case of NFType is SMF and if provided.
fqdn	String	O	0..1	FQDN of the Network Function.
interPlmnFqdn	String	O	0..1	If the NF needs to be discoverable by other NFs in a different PLMN, then an FQDN that is used for inter-PLMN routing.
ipv4Addresses	array(String)	O	0..N	IPv4 address(es) of the Network Function.
priority	Integer	O	0..1	Priority (relative to other NFs of the same type) in the range of 0-65535, to be used for NF selection; lower values indicate a higher priority.
locality	String	O	0..1	Operator defined information about the location of the NF instance.
udmInfo	UDMInfo	O	0..1	Specific data for the UDM (ranges of SUPI, group ID…)
ausfInfo	AUSFInfo	O	0..1	Specific data for the AUSF (ranges of SUPI, group ID…)
amfInfo	AMFInfo	O	0..1	Specific data for the AMF (AMF Set ID, …)
smfInfo	SMFInfo	O	0..1	Specific data for the SMF (DNN's, …).
pcfInfo	PCFInfo	O	0..1	Specific data for the PCF
chfInfo	CHFInfo	O	0..1	Specific data for the CHF

Table 3-26 (Cont.) Configuring NFProfile

Attribute name	Data type	P	Cardinality	Description
nfServices	array(NF Service)	O	0..N	List of NF Service Instances. It includes the services produced by the NF that can be discovered by other NFs, if any.
servingScope	String	O	0..1	If not provided it is taken as "default". It must lie under servingScope of SCP or else the Profile would be rejected. If servingScope of SCP is not provided, it must be left empty. If servingScope of SCP is provided, then it must be set to any one of the configured servingScope. **Note**: servingScope is SCP introduced parameter and used only for NRF profiles or Statically configured profiles.

Configuring UDMInfo

Following are the minimum information required by SCP for statically configuring UDMInfo.

Note: All the below mentioned parameters are according to spec 3GPP TS 29.510 and any parameters other than below mentioned are not used in SCP.

Table 3-27 Configuring UDMInfo

Attribute name	Data type	P	Cardinality	Description
supiRanges	array(SupiRange)	O	0..N	List of ranges of SUPI's whose profile data is available in the UDM instance.
gpsiRanges	arrray(IdentityRange)	O	0..N	List of ranges of GPSIs whose profile data is available in the UDM instance.

Configuring AUSFInfo

Following are the minimum information required by SCP for statically configuring AUSFInfo.

Note: All the below mentioned parameters are according to spec 3GPP TS 29.510 and any parameters other than below mentioned are not used in SCP.

Table 3-28 Configuring AUSFInfo

Attribute name	Data type	P	Cardinality	Description
supiRanges	array(SupiRange)	O	1..N	List of ranges of SUPIs that can be served by the AUSF instance. If not provided, the AUSF can serve any SUPI.

Table 3-28 (Cont.) Configuring AUSFInfo

Attribute name	Data type	P	Cardinality	Description
routingIndicators	array(String)	O	0..N	List of Routing Indicator information that allows to route network signalling with SUCI (see 23.003 [12]) to the AUSF instance. If not provided, the AUSF can serve any Routing Indicator.
GroupId	String	O	0..1	Identity of the AUSF group. If not provided, the AUSF instance does not pertain to any AUSF group.

Configuring AMFInfo

Following are the minimum information required by SCP for statically configuring AMFInfo.

Note: All the below mentioned parameters are according to spec 3GPP TS 29.510 and any parameters other than below mentioned are not used in SCP.

Table 3-29 Configuring AMFInfo

Attribute name	Data type	P	Cardinality	Description
guamiList	array(Guami)	M	1..N	List of supported GUAMIs

Configuring SMFInfo

Following are the minimum information required by SCP for statically configuring SMFInfo.

Note: All the below mentioned parameters are according to spec 3GPP TS 29.510 and any parameters other than below mentioned are not used in SCP.

Table 3-30 Configuring SMFInfo

Attribute name	Data type	P	Cardinality	Description
sNssaiSmfInfoList	array(SnssaiSmfInfoItem)	M	1..N	List of parameters supported by the SMF per S-NSSAI.
pgwFqdn	String	O	0..1	The FQDN of the PGW if the SMF is a combined SMF/PGW-C
accessType	array(AccessType)	O	0..N	If included, this IE shall contain the access type (3GPP_ACCESS and/or NON_3GPP_ACCESS) supported by the SMF. If not included, it is assumed the both access types are supported.

Configuring PCFInfo

Following are the minimum information required by SCP for statically configuring PCFInfo.

Note: All the below mentioned parameters are according to spec 3GPP TS 29.510 and any parameters other than below mentioned are not used in SCP.

Table 3-31 Configuring PCFInfo

Attribute name	Data type	P	Cardinality	Description
supiRanges	array(SupiRange)	O	1..N	List of ranges of SUPIs that can be served by the PCF instance. If not provided, the PCF can serve any SUPI.

Configuring CHFInfo

Following are the minimum information required by SCP for statically configuring CHFInfo.

Note: All the below mentioned parameters are according to spec 3GPP TS 29.510 and any parameters other than below mentioned are not used in SCP.

Table 3-32 Configuring CHFInfo

Attribute name	Data type	P	Cardinality	Description
supiRangeList	array(SupiRange)	O	1..N	List of ranges of SUPIs that can be served by the CHF instance. If not provided, the CHF can serve any SUPI.
gpsiRangeList	arrray(IdentityRange)	O	0..N	List of ranges of GPSI that can be served by the CHF instance. If not provided, the CHF can serve any GPSI.

Configuring NFService

Following are the minimum information required by SCP for statically configuring NFService.

Note: All the below mentioned parameters are according to spec 3GPP TS 29.510 and any parameters other than below mentioned are not used in SCP.

Table 3-33 Configuring NFService

Attribute name	Data type	P	Cardinality	Description
serviceInstanceId	String	M	1	Unique ID of the service instance within a given NF Instance
serviceName	Service Name	M	1	Name of the service instance (e.g. "udm-sdm")

Table 3-33 (Cont.) Configuring NFService

Attribute name	Data type	P	Cardinality	Description
nfServiceStatus	NFServiceStatus	M	1	Status of the NF Service Instance
versions	array(NFServiceVersion)	M	1..N	The API versions supported by the NF Service and if available, the corresponding retirement date of the NF Service.
scheme	UriScheme	M	1	URI scheme (e.g. "http", "https"). **Note**: Only HTTP is supported currently.
fqdn	String	O	0..1	FQDN of the NF Service Instance
ipEndPoints	array(IpEndPoint)	O	0..N	IP address(es) and port information of the Network Function (including IPv4 and/or IPv6 address) where the service is listening for incoming service requests. **Note**: IPV4 is supported currently
apiPrefix	String	O	0..1	Optional path segment(s) used to construct the {apiRoot} variable of the different API URIs, as described in 3GPP 29.501 [5], clause 4.4.1.
priority	Integer	O	0..1	Priority (relative to other services of the same type) in the range of 0-65535, to be used for NF Service selection; lower values indicate a higher priority.
capacity	Integer	O	0..1	Static capacity information in the range of 0-65535, expressed as a weight relative to other services of the same type.
load	Integer	O	0..1	Dynamic load information, ranged from 0 to 100, indicates the current load percentage of the NF Service.

4
Configuring SCP using CNC Console

The REST API configurations can also be performed using Cloud Native Core Console. This section explains the procedure to configure SCP using CNC Console.

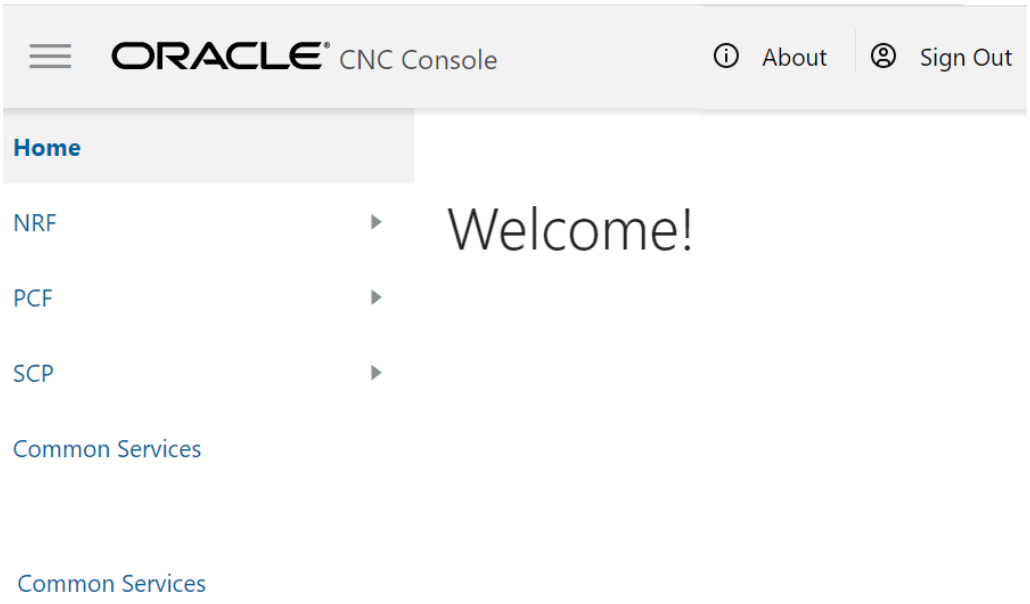
CNC Console Interface

CNC Console Login

Following is the procedure to login to CNC Console:

1. Open any browser.
2. Enter the URL: ***http://<host name>:<port number>***.
3. Enter valid credentials.
4. Click **Log in**. The CNC Console interface is displayed.

Figure 4-1 CNC Console



Top Ribbon

The top ribbon has following options:

1. About
2. Sign Out
3. Help

> **Note:**
>
> The Collapse button at the left side allows the user to collapse the left pane. Help navigates to the swagger.

Left Pane - NFs and APIs

The left pane displays the list of Network Functions and respective APIs.

Right Pane - Details View

The right pane displays details of the parameters that can be updated in the selected API.

Configuring CanaryRelease

Following is the procedure to configure CanaryRelease parameters:

1. From the left navigation menu, navigate to **SCP > Canary Release**. Select **Canary Release**.
2. Click **Edit** to edit or update a Canary Release service parameter. The **Edit Canary Release** Screen appears.
3. Enter the required values. Refer to Configuring CanaryRelease Options for more information on the parameters.
4. Click **Save**.
5. Click **Refresh** to view the updated values on the screen.

Configuring Mediation

Following is the procedure to configure mediation parameters.

Adding Mediation Configuration

1. From the left navigation menu, navigate to **SCP > Mediation Configuration**.
2. Click **Add** from the top bar of the Mediation Configuration screen.
3. Enter the required values. Refer to Configuring Mediation Options for more information on parameter details.
4. Click **Save**.

Editing Mediation Configuration

1. From the left navigation menu, navigate to **SCP > Mediation Configuration**.
2. Click **Edit** against the parameter which must be modified.
3. Click **Save** after performing the modifications.

Deleting Mediation Configuration

1. From the left navigation menu, navigate to **SCP > Mediation Configuration**.
2. Click **Delete** against the parameter which must be deleted.

3. Click **OK** when the message *" Do you want to delete the record"* appears.
4. Click **Refresh** to view the updated values on the screen.

Configuring Message Priority

Following is the procedure to configure mediation parameters.

1. From the left navigation menu, navigate to **SCP > Message Priority**. Select **Message Priority**.
2. Click **Edit** to edit or update a Message Priority parameter. The **Edit Canary Release** Screen appears.
3. Enter/Modify the required values. Refer to Configuring MessagePriority Options for more information on the parameters.
4. Click **Save**.
5. Click **Refresh** to view the updated values on the screen.

Configuring Routing Options

Following is the procedure to configure Routing options parameters:

1. From the left navigation menu, navigate to **SCP > Routing Options**. Select **Routing Options**.
2. Click **Edit** to edit or update a Routing options parameter. The **Edit Routing Options** Screen appears.
3. Enter/Modify the required values. Refer to Configuring Routing Options for more information on the parameters.
4. Click **Save**.
5. Click **Refresh** to view the updated values on the screen.

Configuring SCP Profile

Following is the procedure to configure SCP Profile parameters:

Editing SCP Profile

1. From the left navigation menu, navigate to **SCP > SCP Profile**.
2. Click **Edit**. The **Edit SCP Profile** Screen appears.

> **Note:**
>
> To add a new location to Remaining Localities and Serving Localities type the new location name and click on **Enter** key.

3. Click **Save** after performing the modifications.

Adding NF Services

1. From the left navigation menu, navigate to **SCP > SCP Profile**.

2. Click **Add** from the top bar of the NF Services table.
3. Enter the required values. Refer to Configuring NF Service Groups for more information on parameter details.
4. Click **Save**.

Deleting Mediation Configuration

1. From the left navigation menu, navigate to **SCP > Mediation Configuration**.
2. Click **Delete** against the parameter which must be deleted.
3. Click **Refresh** to view the updated values on the screen.

Configuring Service Groups parameters

Following is the procedure to configure Service Groups parameters:

1. From the left navigation menu, navigate to **SCP > Service Groups**.
2. Click **Edit** from Actions to modify the service groups. The **Edit Service Groups** Screen appears.

> **Note:**
>
> To add a new location to Primary Region Localities and Secondary Region Localities type the new location name and click on Enter key.

3. Click **Save** after performing the modifications.

Configuring System Options

Following is the procedure to configure System Options parameters:

1. From the left navigation menu, navigate to **SCP > System Options**.
2. Click **Edit** from Actions to modify the service groups. The **Edit System Options** Screen appears.
   - CB and OD Enabled
   - HTTP2 Max Requests
   - Connection Timeout
   - Consecutive Errors
   - Interval
   - Base Ejection Time
   - Max Ejection Percent
3. Click **Save** after performing the modifications.

5
Alerts, Metrics and Traces

This section provides the information for Alerts, Metrics and Traces.

Alerts

This section provides information about configuring alerts and supported alerts.

Configuring Alerts

You can configure Alerts in Prometheus and SCPAlertrules.yaml file.

The following table provides information for Alerts for Service Communication Proxy.

Table 5-1 Alert Reference

Alert Name	Severity	Condition	OID used for SNMP Traps	Description
SCPIngressTrafficRateAboveMinorThreshold	minor	sum(rate(ocscp_metric_total_http_rx_req{app_kubernetes_io_name="scp-worker"}[2m]))by (kubernetes_namespace,ocscp_locality,kubernetes_pod_name)>= 1200 < 1400	1.3.6.1.4.1.323.5.3.35.1.2.7001	Notify that Traffic rate is above 1200mps (user configure minor threshold value) with Locality and current value of traffic rate.
SCPIngressTrafficRateAboveMajorThreshold	major	sum(rate(ocscp_metric_total_http_rx_req{app_kubernetes_io_name="scp-worker"}[2m]))by (kubernetes_namespace,ocscp_locality,kubernetes_pod_name) >= 1400 < 1600	1.3.6.1.4.1.323.5.3.35.1.2.7001	Notify that Traffic rate is above 1400mps (user configure major threshold value) with Locality and current value of traffic rate.

Table 5-1 (Cont.) Alert Reference

Alert Name	Severity	Condition	OID used for SNMP Traps	Description
SCPIngressTrafficRateAboveCriticalThreshold	Critical	sum(rate(ocscp_metric_total_http_rx_req{app_kubernetes_io_name="scp-worker"}[2m]))by(kubernetes_namespace, ocscp_locality,kubernetes_pod_name) >= 1600	1.3.6.1.4.1.323.5.3.35.1.2.7001	Notify that Traffic rate is above 1600mps (user configure critical threshold value) with Locality and current value of traffic rate.
SCPRoutingFailedForService	Info	idelta(ocscp_metric_total_routing_send_fail{app_kubernetes_io_name="scp-worker",ocscp_nf_service_type!="Scpc-pilot"}[5m]) > 0	1.3.6.1.4.1.323.5.3.35.1.2.7005	Notify that Routing failed for service. Provides detail like NFService Type, NFType, Locality, and value.
SCPSoothsayerNotificationPodMemoryUsage	major	sum(container_memory_usage_bytes{image!="",pod_name=~".*scpc-notification.+"}) by (pod_name,namespace, instance) > 3006477107	1.3.6.1.4.1.323.5.3.35.1.2.3001	Notify Notification service Pod memory usage if it is above threshold Threshold value is 70% of allocated (4GB) memory: **2.8 GB**
SCPWorkerPodMemoryUsage	major	sum(container_memory_usage_bytes{image!="",pod_name=~".*scp-worker.+"}) by (pod_name,namespace, instance) > 6012954214	1.3.6.1.4.1.323.5.3.35.1.2.7004	Notify Worker per Pod memory usage is above threshold Threshold value is 70% of allocated (8GB) memory: **5.6 GB**
SCPPilotPodMemoryUsage	major	sum(container_memory_usage_bytes{image!="",pod_name=~".*scpc-pilot.+"}) by (pod_name,namespace, instance) > 4509715660	1.3.6.1.4.1.323.5.3.35.1.2.5001	Notify Pilot per Pod memory usage is above threshold Threshold value is 70% of allocated (6GB) memory: **4.2 GB**

Table 5-1 (Cont.) Alert Reference

Alert Name	Severity	Condition	OID used for SNMP Traps	Description
SCPIngressGatewayPodMemoryUsage	major	sum(container_memory_usage_bytes{image!="",pod_name=~".*ingress-gateway.+"}) by (pod_name,namespace, instance) > 2147483648	1.3.6.1.4.1.323.5.3.35.1.2.7010	Notify Ingress Gateway per Pod memory usage is above threshold Threshold value is 50% of allocated (4GB) memory: **2 GB**
SCPInstanceDown	Critical	kube_pod_status_ready{pod =~ '.*scp.*|.*ingress-gateway.*',condition=~ 'true'} !=1	1.3.6.1.4.1.323.5.3.35.1.2.7006	Notify that if any pod in ocscp release is down. Provides information like pod name, instance id and app name.
SCPSoothsayerAuditErrorResponse	Info	scp_soothsayer_audit_error_response > 0	1.3.6.1.4.1.323.5.3.35.1.2.4001	Alert is generated when Audit module receives a 3xx,4xx or 5xx error from NRF. Alert is labeled with specific nftype, servingscope and auditmethod. Alert is cleared on next Audit cycle.

Table 5-1 (Cont.) Alert Reference

Alert Name	Severity	Condition	OID used for SNMP Traps	Description
SCPSoothsayerAuditEmptyNFArrayResponse	Critical	scp_soothsayer_audit_2xx_empty_nf_array > 0	1.3.6.1.4.1.323.5.3.35.1.2.4002	Alert is generated when Audit module receives a 2xx response with empty NFInstance array from NRF. Alert is labeled with specific nftype, servingscope and auditmethod. Alert is cleared if Audit receives a success response with non-empty NFInstance array or on next audit cycle if topology source is changed to LOCAL.
MediationServiceNotAvailable	Critical	idelta(ocscp_metric_total_app_res{app_kubernetes_io_name="scp-worker",ocscp_app_name="nmediation-http",ocscp_response_code="503"}[2m]) > 0	1.3.6.1.4.1.323.5.3.35.1.2.7008	This alert will be generated when SCP receives a '503' response from mediation service.
MediationProcessingFailure	Info	idelta(ocscp_metric_total_mediation_processing_failures{app_kubernetes_io_name="scp-worker"}[2m]) > 0	1.3.6.1.4.1.323.5.3.35.1.2.7009	This alert will be generated when SCP receives a response from mediation service indicating some kind of failure in rules processing at mediation service. For example, JSON parsing error, error in rules application.

Table 5-1 (Cont.) Alert Reference

Alert Name	Severity	Condition	OID used for SNMP Traps	Description
NFInstanceConnectionDown	info	sum(hosts_cx_active{cluster_name!~".*pilot.*|.*jaeger.*|.*prometheus.*|.*elasticsearch.*|.*tiller.*|.*grafana.*|.*snmp-notifier.*|.*kibana.*|.*scpc-.*|.*metric-server.*|.*coredns.*|.*mysql.*|.*scp-worker.*|.*ingress-gateway.*"}) by (endpoint, cluster_name) == 0	1.3.6.1.4.1.323.5.3.35.1.2.7007	Alert will be generated when any upstream connection goes down.

Note:

All metrics operated on namespace of the Service Communication Proxy are deployed. You must configure **scp** namespace when configuring SCPAlertRule.yaml.

Configuring Service Communication Proxy Alert in Prometheus

SCP Helm Chart Release Name: _NAME_

Prometheus NameSpace: _Namespace _

To configure Service Communication Proxy Alert in Prometheus follow the procedure mentioned in Table 5-2.

Table 5-2 Configuring Service Communication Proxy Alert in Prometheus

Step No.	Procedure	Description

1.	Check the name of the config map	To check the name of the config map used by Prometheus use below command:
		
		`$kubectl get configmap -n <_Namespace_>`
		`Example:`
		`$kubectl get configmap -n prometheus-alert2`
		`NAME`
		`DATA AGE`
		`lisa-prometheus-alert2-alertmanager`
		`1 146d`
		`lisa-prometheus-alert2-server`
		`4 146d`

2.	Take backup of current config map	Select the map name appended with " -server ". In above example its " lisa-prometheus-alert2-server " and take its backup using below command:
		
		`# Take Backup of current config map of Prometheus. This command will save the configmap in the provided file. In below command /tmp/tempConfig.yaml is the file where the configmap will get stored.`
		`$ kubectl get configmaps <_NAME_>-server -o yaml -n <_Namespace_> /tmp/tempConfig.yaml`
		`Example:`
		`$ kubectl get configmaps lisa-prometheus-alert2-server -o yaml -n prometheus-alert2 > /tmp/tempConfig.yaml`

3.	Check and delete "alertsscp" rule	Check and delete "alertsscp" rule if its already configured in the prometheus config map. If configured this step will delete the " alertsscp " rule. This is optional step if doing for the first time. `$ sed -i '/etc\/config\/alertsscp/d' /tmp/tempConfig.yaml`
4.	Add the "alertsscp" rule	Add the "alertsscp" rule in the configmap dump file under ' rule_files ' tag. `$ sed -i '/rule_files:/a\ \- /etc/config/alertsscp' /tmp/tempConfig.yaml`

Table 5-2 (Cont.) Configuring Service Communication Proxy Alert in Prometheus

Step No.	Procedure	Description

5.	Update the configmap	Update the configmap using below command. Ensure to use same configmap name which was used to take backup of prometheus configmap in step 2.
		
		`# Update Config map with updated file name of SCP alert file`
		`$ kubectl replace configmap <_NAME_>-server -f /tmp/tempConfig.yaml`
		`Example:`
		`$ kubectl replace configmap lisa-prometheus-alert2-server -f /tmp/tempConfig.yaml`

6.	Add scpAlertrules in configmap	Patch the configmap with new "alertsscp" rule using below command. Kindly note the patch file provided is the custom template file provided with SCP (i.e SCPAlertrules.yaml).
		
		`# Add scpAlertrules in Config map under file name of SCP alert file`
		`$ kubectl patch configmap _NAME_-server -n _Namespace_ --type merge --patch "$(cat ~/SCPAlertrules.yaml)"`
		`Example`
		`$ kubectl patch configmap lisa-prometheus-alert2-server -n prometheus-alert2 --type merge --patch "$(cat ~/SCPAlertrules.yaml)"`

Note:

Prometheus takes nearly 20 seconds to apply the updated Config map.

Configuring Service Communication Proxy Alert using SCPAlertrules.yaml file

Note:

Default NameSpace is **scpsvc** for Service Communication Proxy. You can update the namespace as per the deployment.

Following is a sample yaml file.

```
apiVersion: v1
data:
  alertsscp: |
    groups:
    - name: SCPAlerts
      rules:
         #Alerts for SCP Ingress Traffic Rate, it uses namespace of spc
deployed
      - alert: SCPIngressTrafficRateAboveMinorThreshold
        annotations:
          description: 'Ingress Traffic Rate at locality:
"{{$labels.ocscp_locality}}"  is above minor threshold (i.e. 1200 mps)'
          summary: 'namespace: {{$labels.kubernetes_namespace}},
podname: {{$labels.kubernetes_pod_name}}, timestamp: {{ with query
"time()" }}{{ . | first | value | humanizeTimestamp }}{{ end }}:
Current Ingress Traffic Rate is {{ $value | printf "%.2f" }} mps which
is above 70 Percent of Max MPS(1700)'
         # Provide app and kubernetes_namespace of scp deployed
        expr:
sum(rate(ocscp_metric_total_http_rx_req{app_kubernetes_io_name="scp-
worker"}[2m])) by
(kubernetes_namespace,ocscp_locality,kubernetes_pod_name) >= 1200 < 1400
        for: 1m
        labels:
          severity: minor
          alertname: "SCPIngressTrafficRateAboveMinorThreshold"
          oid: "1.3.6.1.4.1.323.5.3.35.1.2.7001"
          namespace: ' {{ $labels.kubernetes_namespace }} '
          podname: ' {{$labels.kubernetes_pod_name}} '
          vendor: oracle
      - alert: SCPIngressTrafficRateAboveMajorThreshold
        annotations:
          timestamp: ' {{ with query "time()" }}{{ . | first | value |
humanizeTimestamp }}{{ end }} '
          description: 'Ingress Traffic Rate at locality:
{{$labels.ocscp_locality}} is above major threshold (i.e. 1400 mps)'
          summary: 'namespace: {{$labels.kubernetes_namespace}},
podname: {{$labels.kubernetes_pod_name}}, timestamp: {{ with query
"time()" }}{{ . | first | value | humanizeTimestamp }}{{ end }}:
Current Ingress Traffic Rate is {{ $value | printf "%.2f" }} mps which
is above 80 Percent of Max MPS(1700)'
         # Provide app and kubernetes_namespace of scp deployed
        expr:
sum(rate(ocscp_metric_total_http_rx_req{app_kubernetes_io_name="scp-
worker"}[2m])) by
(kubernetes_namespace,ocscp_locality,kubernetes_pod_name)  >= 1400 <
1600
        for: 1m
        labels:
          severity: major
          alertname: "SCPIngressTrafficRateAboveMajorThreshold"
          oid: "1.3.6.1.4.1.323.5.3.35.1.2.7001"
          namespace: ' {{ $labels.kubernetes_namespace }} '
```

```
          podname: ' {{$labels.kubernetes_pod_name}} '
          vendor: oracle
      - alert: SCPIngressTrafficRateAbovecriticalThreshold
        annotations:
          description: 'Ingress Traffic Rate at locality:
{{$labels.ocscp_locality}} is above critical threshold (i.e. 1600 mps)'
          summary: 'namespace: {{$labels.kubernetes_namespace}},
podname: {{$labels.kubernetes_pod_name}}, timestamp: {{ with query
"time()" }}{{ . | first | value | humanizeTimestamp }}{{ end }}:
Current Ingress Traffic Rate is {{ $value | printf "%.2f" }} mps which
is above 95 Percent of Max MPS(1700)'
         # Provide app and kubernetes_namespace of scp deployed
        expr:
sum(rate(ocscp_metric_total_http_rx_req{app_kubernetes_io_name="scp-
worker"}[2m])) by
(kubernetes_namespace,ocscp_locality,kubernetes_pod_name) >= 1600
        for: 1m
        labels:
          severity: critical
          alertname: "SCPIngressTrafficRateAbovecriticalThreshold"
          oid: "1.3.6.1.4.1.323.5.3.35.1.2.7001"
          namespace: ' {{ $labels.kubernetes_namespace }} '
          podname: ' {{$labels.kubernetes_pod_name}} '
          vendor: oracle
      - alert: SCPRoutingFailedForService
        annotations:
          description: 'Routing failed for nfservicetype:
{{$labels.ocscp_nf_service_type}}'
          summary: 'Routing failed for service: nfservicetype =
{{$labels.ocscp_nf_service_type}}, nfserviceinstanceid =
{{$labels.ocscp_service_instance_id}}, nftype =
{{$labels.ocscp_nf_type}}, nfinstanceid =
{{$labels.ocscp_nf_instance_id}}, locality =
{{$labels.ocscp_locality}}, nfendpoint =
{{$labels.ocscp_nf_end_point}}, namespace:
{{$labels.kubernetes_namespace}}, podname:
{{$labels.kubernetes_pod_name}}, timestamp: {{ with query "time()" }}
{{ . | first | value | humanizeTimestamp }}{{ end }} and value =
{{ $value }} '
         # Provide app and kubernetes_namespace of scp deployed
        expr:
idelta(ocscp_metric_total_routing_send_fail{app_kubernetes_io_name="scp-
worker",ocscp_nf_service_type!="Scpc-pilot"}[5m]) > 0
        labels:
          severity: info
          alertname: "SCPRoutingFailedForService"
          oid: "1.3.6.1.4.1.323.5.3.35.1.2.7005"
          namespace: ' {{ $labels.kubernetes_namespace }} '
          podname: ' {{$labels.kubernetes_pod_name}} '
          nfservicetype: ' {{$labels.ocscp_nf_service_type}} '
          nfendpoint: ' {{$labels.ocscp_nf_end_point}} '
          nfserviceinstanceid: ' {{$labels.ocscp_service_instance_id}} '
          nfinstanceid: ' {{$labels.ocscp_nf_instance_id}} '
          vendor: oracle
      - alert: SCPSoothsayerNotificationPodMemoryUsage
```

```
         # Provide kubernetes_namespace of scp deployed and pod name
substring as its regex match of pod name
        expr: sum(container_memory_usage_bytes{image!
="",pod_name=~"scpc-notification.+"})  by (pod_name,namespace,
instance) > 3006477107
        for: 2m
        labels:
          severity: major
          alertname: "SCPSoothsayerNotificationPodMemoryUsage"
          oid: "1.3.6.1.4.1.323.5.3.35.1.2.3001"
          namespace: ' {{ $labels.namespace }} '
          podname: ' {{$labels.pod_name}} '
          vendor: oracle
        annotations:
          description: 'instancename: {{$labels.instance}}, namespace:
{{$labels.namespace}}, podname: {{$labels.pod_name}}: Soothsayer
Notification Pod High Memory usage detected'
          summary: 'instancename: {{$labels.instance}}, namespace:
{{$labels.namespace}}, podname: {{$labels.pod_name}}, timestamp:
{{ with query "time()" }}{{ . | first | value | humanizeTimestamp }}
{{ end }}: Memory usage is above 70% (current value is: {{ $value }})'
      - alert: SCPWorkerPodMemoryUsage
         # Provide kubernetes_namespace of scp deployed and pod name
substring as its regex match of pod name
        expr: sum(container_memory_usage_bytes{image!="",pod_name=~"scp-
worker.+"})  by (pod_name,namespace, instance) > 6012954214
        for: 2m
        labels:
          severity: major
          alertname: "SCPWorkerPodMemoryUsage"
          oid: "1.3.6.1.4.1.323.5.3.35.1.2.7004"
          namespace: ' {{ $labels.namespace }} '
          podname: ' {{$labels.pod_name}} '
          vendor: oracle
        annotations:
          description: 'instancename: {{$labels.instance}}, namespace:
{{$labels.namespace}}, podname: {{$labels.pod_name}}: Worker Pod High
Memory usage detected'
          summary: 'instancename: {{$labels.instance}}, namespace:
{{$labels.namespace}}, podname: {{$labels.pod_name}}, timestamp:
{{ with query "time()" }}{{ . | first | value | humanizeTimestamp }}
{{ end }}: Memory usage is above 70% (current value is: {{ $value }})'
      - alert: SCPPilotPodMemoryUsage
         # Provide kubernetes_namespace of scp deployed and pod name
substring as its regex match of pod name
        expr: sum(container_memory_usage_bytes{image!="",pod_name=~"scp-
pilot.+"})  by (pod_name,namespace, instance)  > 4509715660
        for: 5m
        labels:
          severity: major
          alertname: "SCPPilotPodMemoryUsage"
          oid: "1.3.6.1.4.1.323.5.3.35.1.2.5001"
          namespace: ' {{ $labels.namespace }} '
          podname: ' {{$labels.pod_name}} '
          vendor: oracle
```

```
        annotations:
          description: 'instancename: {{$labels.instance}}, namespace:
{{$labels.namespace}}, podname: {{$labels.pod_name}}: Pilot Pod High
Memory usage detected'
          summary: 'instancename: {{$labels.instance}}, namespace:
{{$labels.namespace}}, podname: {{$labels.pod_name}}, timestamp:
{{ with query "time()" }}{{ . | first | value | humanizeTimestamp }}
{{ end }}: Memory usage is above 70% (current value is: {{ $value }})'
      - alert: SCPIngressGatewayPodMemoryUsage
         # Provide kubernetes_namespace of scp deployed and pod name
substring as its regex match of pod name
        expr: sum(container_memory_usage_bytes{image!
="",pod_name=~".*ingress-gateway.+"}) by (pod_name,namespace, instance)
> 2147483648
        for: 5m
        labels:
          severity: major
          alertname: "SCPIngressGatewayPodMemoryUsage"
          oid: "1.3.6.1.4.1.323.5.3.35.1.2.7010"
          namespace: ' {{ $labels.namespace }} '
          podname: ' {{$labels.pod_name}} '
          vendor: oracle
        annotations:
          description: 'instancename: {{$labels.instance}}, namespace:
{{$labels.namespace}}, podname: {{$labels.pod_name}}: SCP Ingress
Gateway Pod High Memory usage detected'
          summary: 'instancename: {{$labels.instance}}, namespace:
{{$labels.namespace}}, podname: {{$labels.pod_name}}, timestamp:
{{ with query "time()" }}{{ . | first | value | humanizeTimestamp }}
{{ end }}: Memory usage is above 50% (current value is: {{ $value }})'
      - alert: SCPInstanceDown
        expr: kube_pod_status_ready{pod =~ '.*scp.*|.*ingress-
gateway.*',condition =~ 'true'} !=1
        for: 2m
        labels:
          severity: critical
          oid: "1.3.6.1.4.1.323.5.3.35.1.2.7006"
          namespace: '{{ $labels.kubernetes_namespace }} '
          podname: ' {{ $labels.kubernetes_pod_name }} '
          vendor: oracle
        annotations:
          description: 'Pod with podname:
{{$labels.kubernetes_pod_name}}, instancename: {{$labels.instance}},
appname: {{$labels.app}} has been down for more than 2 minutes'
          summary: 'Pod with podname: {{$labels.kubernetes_pod_name}},
instancename: {{$labels.instance}}, appname: {{$labels.app}},
timestamp: {{ with query "time()" }}{{ . | first | value |
humanizeTimestamp }}{{ end }} is Down '
      - alert: NFInstanceConnectionDown
        expr: sum(hosts_cx_active{cluster_name!
~".*pilot.*|.*jaeger.*|.*prometheus.*|.*elasticsearch.*|.*tiller.*|.*gra
fana.*|.*snmp-notifier.*|.*kibana.*|.*scpc-.*|.*metric-
server.*|.*coredns.*|.*mysql.*|.*scp-worker.*|.*ingress-gateway.*"}) by
(endpoint, cluster_name) == 0
        labels:
```

```
          severity: info
          oid: "1.3.6.1.4.1.323.5.3.35.1.2.7007"
          namespace: '{{ $labels.kubernetes_namespace }} '
          podname: ' {{ $labels.kubernetes_pod_name }} '
          nfendpoint: ' {{ $labels.endpoint }} '
          nfclustername: ' {{ $labels.cluster_name }} '
          vendor: oracle
        annotations:
          description: 'Connection down with IP Endpoint:
{{$labels.endpoint}}, clustername: {{$labels.cluster_name}}'
          summary: 'Connection down with IP Endpoint:
{{$labels.endpoint}}, clustername: {{$labels.cluster_name}}'
      - alert: SCPSoothsayerAuditErrorResponse
        expr: scp_soothsayer_audit_error_response > 0
        labels:
          severity: info
          alertname: "SCPSoothsayerAuditErrorResponse"
          oid: "1.3.6.1.4.1.323.5.3.35.1.2.4001"
          namespace: ' {{ $labels.kubernetes_namespace }} '
          podname: ' {{$labels.kubernetes_pod_name}} '
          vendor: oracle
        annotations:
          description: 'SCP Audit received Error response for nftype
{{$labels.nftype}}'
          summary: 'SCP Audit received Error response for nftype
{{$labels.nftype}}, servingscope: {{$labels.servingscope}},
auditmethod: {{$labels.auditmethod}}, namespace:
{{$labels.kubernetes_namespace}}, podname:
{{$labels.kubernetes_pod_name}}, timestamp: {{ with query "time()" }}
{{ . | first | value | humanizeTimestamp }}{{ end }}'
      - alert: SCPSoothsayerAuditEmptyNFArrayResponse
        expr: scp_soothsayer_audit_2xx_empty_nf_array > 0
        labels:
          severity: critical
          alertname: "SCPSoothsayerAuditEmptyNFArrayResponse"
          oid: "1.3.6.1.4.1.323.5.3.35.1.2.4002"
          namespace: ' {{ $labels.kubernetes_namespace }} '
          podname: ' {{$labels.kubernetes_pod_name}} '
          vendor: oracle
        annotations:
          description: 'SCP Audit received Empty NF Array Response for
nftype {{$labels.nftype}}'
          summary: 'SCP Audit received Empty NF Array Response for
nftype {{$labels.nftype}}, servingscope: {{$labels.servingscope}},
auditmethod: {{$labels.auditmethod}}, namespace:
{{$labels.kubernetes_namespace}}, podname:
{{$labels.kubernetes_pod_name}}, timestamp: {{ with query "time()" }}
{{ . | first | value | humanizeTimestamp }}{{ end }}'
      - alert: MediationServiceNotAvailable
        annotations:
          description: 'Mediation service not available'
          summary: 'Mediation Service is not available: triggerpoint =
{{$labels.ocscp_trigger_name}}, nfservicetype =
{{$labels.ocscp_nf_service_type}}, nfserviceinstanceid =
{{$labels.ocscp_service_instance_id}}, nftype =
```

```
{{$labels.ocscp_nf_type}}, nfinstanceid =
{{$labels.ocscp_nf_instance_id}}, locality =
{{$labels.ocscp_locality}}, nfendpoint =
{{$labels.ocscp_nf_end_point}}, namespace:
{{$labels.kubernetes_namespace}}, podname:
{{$labels.kubernetes_pod_name}}, timestamp: {{ with query "time()" }}
{{ . | first | value | humanizeTimestamp }}{{ end }} and value =
{{ $value }} '
         # Provide app and kubernetes_namespace of scp deployed
        expr:
idelta(ocscp_metric_total_app_res{app_kubernetes_io_name="scp-
worker",ocscp_app_name="nmediation-http",ocscp_response_code="503"}
[2m]) > 0
        labels:
          severity: critical
          alertname: "SCPMediationServiceNotAvailable"
          oid: "1.3.6.1.4.1.323.5.3.35.1.2.7008"
          namespace: ' {{ $labels.kubernetes_namespace }} '
          podname: ' {{$labels.kubernetes_pod_name}} '
          nfservicetype: ' {{$labels.ocscp_nf_service_type}} '
          nfendpoint: ' {{$labels.ocscp_nf_end_point}} '
          nfserviceinstanceid: ' {{$labels.ocscp_service_instance_id}} '
          nfinstanceid: ' {{$labels.ocscp_nf_instance_id}} '
          triggerpoint: ' {{$labels.ocscp_trigger_name}} '
          vendor: oracle
      - alert: MediationProcessingFailure
        annotations:
          description: 'Processing failure at mediation service'
          summary: 'Mediation service failed to respond properly.
namespace: {{$labels.kubernetes_namespace}}, podname:
{{$labels.kubernetes_pod_name}}, timestamp: {{ with query "time()" }}
{{ . | first | value | humanizeTimestamp }}{{ end }} and value =
{{ $value }} '
         # Provide app and kubernetes_namespace of scp deployed
        expr:
idelta(ocscp_metric_total_mediation_processing_failures{app_kubernetes_i
o_name="scp-worker"}[2m]) > 0
        labels:
          severity: info
          alertname: "SCPMediationProcessingFailure"
          oid: "1.3.6.1.4.1.323.5.3.35.1.2.7009"
          namespace: ' {{ $labels.kubernetes_namespace }} '
          podname: ' {{$labels.kubernetes_pod_name}} '
          vendor: oracle
```

Alerts Details

Description and Summary are added by Prometheus alert manager.

Alerts are supported for three different resources/routing crosses threshold.

- SCPIngress Traffic Rate Above Threshold
  - Has three threshold level Minor (above 1400 mps to 2000mps), Major (1600 to 1800 mps), Critical (above 1800 mps). These values are configurable.

  - In the description, information is presented similar to: "Ingress Traffic Rate at Locality: <Locality of scp> is above <threshold level (minor/major/critical> threshold (i.e. <value of threshold>)"
  - In Summary: "Namespace: <Namespace of scp deployment that Locality>, Pod: <SCP-worker Pod name>: Current Ingress Traffic Rate is <Current rate of Ingress traffic > mps which is above 70 Percent of Max MPS(<upper limit of ingress traffic rate per pod>)"

    > **Note:**
    >
    > Ingress traffic rate is per scp-worker pod in a namespace at particular SCP-Locality. Currently, 2000mps is the upper limit for per scp-worker pod.

- SCP Routing Failed For Service
  - It alerts for which NF Service Type and NF Type at particular locality, Routing failed
  - Description:- "Routing failed for service"
  - Summary: - "Routing failed for service: NFService Type = <Message NF Service Type>, NFType = <Message NF Type>, Locality = <SCP Locality where Routing Failed> and value = <Accumulated failure till now, of such message for NFType and NFService Type>"

    > **Note:**
    >
    > The value field currently does not provide number of failures in particular time interval, instead it provides the total number of Routing failures.

- SCP Pod Memory Usage:- Three type of alerts namely SCPSoothsayerPodMemoryUsage, SCPWorkerPodMemoryUsage, SCPPilotPodMemoryUsage
  - Pod memory usage for SCP Pods (Soothsayer, Worker and Pilot) deployed at a particular node instance is provided.
  - The Soothsayer pod threshold is 8 GB
  - The Worker pod threshold is 4 GB
  - The Pilot pod threshold is 6GB
  - Summary: Instance: "<Node Instance name>, NameSpace: <Namespace of SCP deployment>, Pod: <(Soothsayer/Worker/Pilot) Pod name>: <Soothsayer/Worker/Pilot> Pod High Memory usage detected"
  - Summary: "Instance: "<Node Instance name>, Namespace: <Namespace of SCP deployment>, Pod: <(Soothsayer/Worker/Pilot) Pod name>: Memory usage is above <threshold value>G (current value is: <current value of memory usage>)"

Configuring alert manager for SNMP notifier

Grouping of alerts is based on:

- podname
- alertname
- severity
- namespace
- nfServiceType
- nfServiceInstanceId
- servingscope
- nftype

User needs to add sub-routes for SCP alerts in AlertManager config map as below:

Table 5-3 Alert Manager configuration for SNMP Notifier

Step No#	Procedure	Description

1. ☐	Take Backup of current config map of Alertmanager	Execute the following command:
		
		`kubectl get configmaps _NAME_-alertmanager -oyaml -n _Namespace_ > /tmp/bkupAlertManagerConfig.yaml`
		
		Example:
		
		`kubectl get configmaps occne-prometheus-alertmanager -oyaml -n occne-infra > /tmp/bkupAlertManagerConfig.yaml`

2. ☐	Edit Configmap to add subroute for SCP Trap OID	Execute the following command:
		
		`kubectl edit configmaps _NAME_-alertmanager -n _Namespace_`
		`Example:`
		
		Example:
		
		`kubectl edit configmaps occne-prometheus-alertmanager -n occne-infra`

Table 5-3 (Cont.) Alert Manager configuration for SNMP Notifier

Step No#	Procedure	Description
3. ☐	Add the subroute under 'route' in configmap	routes: - receiver: default-receiver group_interval: 1m group_wait: 10s repeat_interval: 9y group_by: [podname, alertname, severity, namespace, nfservicetype, nfserviceinstanceid, servingscope, nftype] match_re: oid: ^1.3.6.1.4.1.323.5.3.35.(.*)

Metrics Reference

The following table provides information for metrics for Service Communication Proxy.

Table 5-4 Metrics Reference

Prometheus Stat Metric Name	Metric Description	Dimensions	Example usage to filter metric by dimension on Grafana GUI
ocscp_metric_nf_total_http_tx_req	Total number of HTTP requests forwarded by Service Communication Proxy to upstream cluster	• ocscp_nf_type (e.g., UDM, PCF, AMF, etc.) • ocscp_nf_service_type (e.g., nudm-uecm, nudm-sdm, etc.) • ocscp_nf_end_point (Default value = 0.0:00)	• ocscp_metric_nf_total_http_tx_req{ocscp_nf_type="UDM"} • ocscp_metric_nf_total_http_tx_req{ocscp_nf_service_type="nudm-uecm"} • ocscp_metric_nf_total_http_tx_req{ocscp_nf_end_point="10.96.166.65:80"}
ocscp_metric_nf_total_http_rx_req	The total number of incoming HTTP requests	• ocscp_nf_type (e.g., UDM, PCF, AMF, etc.) • ocscp_nf_service_type (e.g., nudm-uecm, nudm-sdm, etc.)	• ocscp_metric_nf_total_http_rx_req{ocscp_nf_type="UDM"} • ocscp_metric_nf_total_http_rx_req{ocscp_nf_service_type="nudm-uecm"}

Table 5-4 (Cont.) Metrics Reference

Prometheus Stat Metric Name	Metric Description	Dimensions	Example usage to filter metric by dimension on Grafana GUI
ocscp_metric_nf_total_http_rx_res	Total number of HTTP response received by SCP with specific HTTP response codes (e.g., 201, 503, etc.)	• ocscp_response_code (e.g., 201, 503, 404, etc.) • ocscp_nf_type (e.g., UDM, PCF, AMF, etc.) • ocscp_nf_service_type (e.g., nudm-uecm, nudm-sdm, etc.) • ocscp_nf_end_point (Default value = 0.0:00)	• ocscp_metric_nf_total_http_rx_res{ocscp_response_code="201"} • ocscp_metric_nf_total_http_rx_res{ocscp_nf_type="UDM"} • ocscp_metric_nf_total_http_rx_res{ocscp_nf_service_type="nudm-uecm"} • ocscp_metric_bf_total_http_rx_res{ocscp_nf_end_point="10.96.166.65:80"}
ocscp_metric_nf_total_http_rx_res_xx	Total number of HTTP response received by SCP with aggregated HTTP response codes (e.g., 2xx, 5xx, etc.)	• ocscp_response_code_class (e.g., 2xx, 5xx, etc.) • ocscp_nf_type (e.g., UDM, PCF, AMF, etc.) • ocscp_nf_service_type (e.g., nudm-uecm, nudm-sdm, etc.) • ocscp_nf_end_point (Default value = 0.0:00)	• ocscp_metric_nf_total_http_rx_res_xx{ocscp_response_code_class="2"} • ocscp_metric_nf_total_http_rx_res_xx{ocscp_nf_type="UDM"} • ocscp_metric_nf_total_http_rx_res_xx{ocscp_nf_service_type="nudm-uecm"} • ocscp_metric_nf_total_http_rx_res_xx{ocscp_nf_end_point="10.96.166.65:80"}
ocscp_metric_nf_total_http_tx_res	Total number of HTTP response forwarded by SCP with specific HTTP response codes (e.g., 201, 503, etc.)	• ocscp_response_code (e.g., 201, 503, 404, etc.) • ocscp_nf_type (e.g., UDM, PCF, AMF, etc.) • ocscp_nf_service_type (e.g., nudm-uecm, nudm-sdm, etc.)	• ocscp_metric_nf_total_http_tx_res{ocspf_response_code="201"} • ocscp_metric_nf_total_http_tx_res{ocspf_nf_type="UDM"} • ocscp_metric_nf_total_http_tx_res{ocspf_nf_service_type="nudm-uecm"}
ocscp_metric_nf_total_http_tx_res_xx	Total number of HTTP response forwarded by SCP with aggregated HTTP response codes (e.g., 2xx, 5xx, etc.)	• ocscp_response_code_class (e.g., 2xx, 5xx, etc.) • ocscp_nf_type (e.g., UDM, PCF, AMF, etc.) • ocscp_nf_service_type (e.g., nudm-uecm, nudm-sdm, etc.)	• ocscp_metric_nf_total_http_tx_res_xx{ocscp_response_code_class="2"} • ocscp_metric_nf_total_http_tx_res_xx{ocscp_nf_type="UDM"} • ocscp_metric_nf_total_http_tx_res_xx{ocscp_nf_service_type="nudm-uecm"}

Table 5-4 (Cont.) Metrics Reference

Prometheus Stat Metric Name	Metric Description	Dimensions	Example usage to filter metric by dimension on Grafana GUI
ocscp_metric_total_http_rx_req	The total number of incoming HTTP requests	• ocscp_nf_type (e.g., UDM, PCF, AMF, etc.) • ocscp_nf_service_type (e.g., nudm-uecm, nudm-sdm, etc.) • ocscp_req_msg_size (The request message size buckets. e.g., 1 (size < 1k bytes), 2 (1k < size < 2k bytes), 4 (2k < size < 4k), etc.) • ocscp_locality (SCP site name e.g., Loc6, Loc7, etc.)	• ocscp_metric_total_http_rx_req{ocscp_nf_type="UDM"} • ocscp_metric_total_http_rx_req{ocscp_nf_service_type="nudm-uecm"} • ocscp_metric_total_http_rx_req{ocscp_req_msg_size="2"} • ocscp_metric_total_http_rx_req{ocscp_locality="Loc7"}
ocscp_metric_total_http_tx_req	Total number of HTTP requests forwarded by Service Communication Proxy to upstream cluster	• ocscp_nf_type (e.g., UDM, PCF, AMF, etc.) • ocscp_nf_service_type (e.g., nudm-uecm, nudm-sdm, etc.) • ocscp_nf_end_point (Default value = 0.0:00) • ocscp_locality (SCP site name e.g., Loc6, Loc7, etc.) • ocscp_nf_instance_id (e.g., 6faf1bbc-6e4a-4454-a507-a14ef8e1bc5c, etc. Default value = NA) • ocscp_service_instance_id (e.g., fe137ab7-740a-46ee-aa5c-951806d77b02, etc. Default value = NA)	• ocscp_metric_total_http_tx_req{ocscp_nf_type="UDM"} • ocscp_metric_total_http_tx_req{ocscp_nf_service_type="nudm-uecm"} • ocscp_metric_total_http_tx_req{ocscp_nf_end_point="10.96.166.65:80"} • ocscp_metric_total_http_tx_req{ocscp_locality="Loc7"} • ocscp_metric_total_http_tx_req{ocscp_nf_instance_id="6faf1bbc-6e4a-4454-a507-a14ef8e1bc5c"} • ocscp_metric_total_http_tx_req{ocscp_service_instance_id="fe137ab7-740a-46ee-aa5c-951806d77b02"}

Table 5-4 (Cont.) Metrics Reference

Prometheus Stat Metric Name	Metric Description	Dimensions	Example usage to filter metric by dimension on Grafana GUI
ocscp_metric_total_http_rx_res	Total number of HTTP response received by SCP with specific HTTP response codes (e.g., 201, 503, etc.)	• ocscp_response_code (e.g., 201, 503, 404, etc.) • ocscp_nf_type (e.g., UDM, PCF, AMF, etc.) • ocscp_nf_service_type (e.g., nudm-uecm, nudm-sdm, etc.) • ocscp_nf_end_point (Default value = 0.0:00) • ocscp_locality (SCP site name e.g., Loc6, Loc7, etc.) • ocscp_nf_instance_id (e.g., 6faf1bbc-6e4a-4454-a507-a14ef8e1bc5c, etc. Default value = NA) • ocscp_service_instance_id (e.g., fe137ab7-740a-46ee-aa5c-951806d77b02, etc. Default value = NA) • ocscp_res_msg_size (The response message size buckets. e.g., 1 (size < 1k bytes), 2 (1k < size < 2k bytes), 4 (2k < size < 4k), etc.)	• ocscp_metric_total_http_rx_res{ocscp_response_code="201"} • ocscp_metric_total_http_rx_res{ocscp_nf_type="UDM"} • ocscp_metric_total_http_rx_res{ocscp_nf_service_type="nudm-uecm"} • ocscp_metric_total_http_rx_res{ocscp_nf_end_point="10.96.166.65:80"} • ocscp_metric_total_http_rx_res{ocscp_locality="Loc7"} • ocscp_metric_total_http_rx_res{ocscp_nf_instance_id="6faf1bbc-6e4a-4454-a507-a14ef8e1bc5c"} • ocscp_metric_total_http_rx_res{ocscp_service_instance_id="fe137ab7-740a-46ee-aa5c-951806d77b02"} • ocscp_metric_total_http_rx_res{ocscp_res_msg_size="2"}

Table 5-4 (Cont.) Metrics Reference

Prometheus Stat Metric Name	Metric Description	Dimensions	Example usage to filter metric by dimension on Grafana GUI
ocscp_metric_total_http_rx_res_xx	Total number of HTTP response received by SCP with aggregated HTTP response codes (e.g., 2xx, 5xx, etc.)	• ocscp_response_code_class (e.g., 2xx, 5xx, etc.) • ocscp_nf_type (e.g., UDM, PCF, AMF, etc.) • ocscp_nf_service_type (e.g., nudm-uecm, nudm-sdm, etc.) • ocscp_nf_end_point (Default value = 0.0:00) • ocscp_locality (SCP site name e.g., Loc6, Loc7, etc.) • ocscp_nf_instance_id (e.g., 6faf1bbc-6e4a-4454-a507-a14ef8e1bc5c, etc. Default value = NA) • ocscp_service_instance_id (e.g., fe137ab7-740a-46ee-aa5c-951806d77b02, etc. Default value = NA)	• ocscp_metric_total_http_rx_res_xx{ocscp_response_code_class="2"} • ocscp_metric_total_http_rx_res_xx{ocscp_nf_type="UDM"} • ocscp_metric_total_http_rx_res_xx{ocscp_nf_service_type="nudm-uecm"} • ocscp_metric_total_http_rx_res_xx{ocscp_nf_end_point="10.96.166.65:80"} • ocscp_metric_total_http_rx_res_xx{ocscp_locality="Loc7"} • ocscp_metric_total_http_rx_res_xx{ocscp_nf_instance_id="6faf1bbc-6e4a-4454-a507-a14ef8e1bc5c"} • ocscp_metric_total_http_rx_res_xx{ocscp_service_instance_id="fe137ab7-740a-46ee-aa5c-951806d77b02"}
ocscp_metric_total_http_tx_res	Total number of HTTP response forwarded by SCP with specific HTTP response codes (e.g., 201, 503, etc.)	• ocscp_response_code (e.g., 201, 503, 404, etc.) • ocscp_nf_type (e.g., UDM, PCF, AMF, etc.) • ocscp_nf_service_type (e.g., nudm-uecm, nudm-sdm, etc.) • ocscp_locality (SCP site name e.g., Loc6, Loc7, etc.)	• ocscp_metric_total_http_tx_res{ocspf_response_code="201"} • ocscp_metric_total_http_tx_res{ocspf_nf_type="UDM"} • ocscp_metric_total_http_tx_res{ocspf_nf_service_type="nudm-uecm"} • ocscp_metric_total_http_tx_res{ocscp_locality="Loc7"}

Table 5-4 (Cont.) Metrics Reference

Prometheus Stat Metric Name	Metric Description	Dimensions	Example usage to filter metric by dimension on Grafana GUI
ocscp_metric_total_http_tx_res_xx	Total number of HTTP response forwarded by SCP with aggregated HTTP response codes (e.g., 2xx, 5xx, etc.)	• ocscp_response_code_class (e.g., 2xx, 5xx, etc.) • ocscp_nf_type (e.g., UDM, PCF, AMF, etc.) • ocscp_nf_service_type (e.g., nudm-uecm, nudm-sdm, etc.) • ocscp_locality (SCP site name e.g., Loc6, Loc7, etc.)	• ocscp_metric_total_http_tx_res_xx{ocscp_response_code_class="2"} • ocscp_metric_total_http_tx_res_xx{ocscp_nf_type="UDM"} • ocscp_metric_total_http_tx_res_xx{ocscp_nf_service_type="nudm-uecm"} • ocscp_metric_total_http_tx_res_xx{ocscp_locality="Loc7"}
ocscp_metric_total_http_rx_messages	Total incoming (rx) messages to SCP. This includes requests and responses.	• ocscp_nf_type (e.g., UDM, PCF, AMF, etc.) • ocscp_nf_service_type (e.g., nudm-uecm, nudm-sdm, etc.) • ocscp_locality (SCP site name e.g., Loc6, Loc7, etc.)	• ocscp_metric_total_http_rx_messages{ocscp_nf_type="UDM"} • ocscp_metric_total_http_rx_messages{ocscp_nf_service_type="nudm-uecm"} • ocscp_metric_total_http_rx_messages{ocscp_locality="Loc7"}

Table 5-4 (Cont.) Metrics Reference

Prometheus Stat Metric Name	Metric Description	Dimensions	Example usage to filter metric by dimension on Grafana GUI
ocscp_metric_total_http_tx_messages	Total outgoing (tx) messages from SCP. This includes requests and responses.	• ocscp_nf_type (e.g., UDM, PCF, AMF, etc.) • ocscp_nf_service_type (e.g., nudm-uecm, nudm-sdm, etc.) • ocscp_nf_end_point (Default value = 0.0:00) • ocscp_locality (SCP site name e.g., Loc6, Loc7, etc.) • ocscp_nf_instance_id (e.g., 6faf1bbc-6e4a-4454-a507-a14ef8e1bc5c, etc. Default value = NA) • ocscp_service_instance_id (e.g., fe137ab7-740a-46ee-aa5c-951806d77b02, etc. Default value = NA)	• ocscp_metric_total_http_tx_messages{ocscp_nf_type="UDM"} • ocscp_metric_total_http_tx_messages{ocscp_nf_service_type="nudm-uecm"} • ocscp_metric_total_http_tx_messages{ocscp_nf_end_point="10.96.166.65:80"} • ocscp_metric_total_http_tx_messages{ocscp_locality="Loc7"} • ocscp_metric_total_http_tx_messages{ocscp_nf_instance_id="6faf1bbc-6e4a-4454-a507-a14ef8e1bc5c"} • ocscp_metric_total_http_tx_messages{ocscp_service_instance_id="fe137ab7-740a-46ee-aa5c-951806d77b02"}

Table 5-4 (Cont.) Metrics Reference

Prometheus Stat Metric Name	Metric Description	Dimensions	Example usage to filter metric by dimension on Grafana GUI
ocscp_metric_total_attempts_to_forward_route	Total number of requests that matched the catch-all-route routing rule.	• ocscp_nf_type (e.g., UDM, PCF, AMF, etc.) • ocscp_nf_service_type (e.g., nudm-uecm, nudm-sdm, etc.) • ocscp_nf_end_point (Default value = 0.0:00) • ocscp_locality (SCP site name e.g., Loc6, Loc7, etc.) • ocscp_nf_instance_id (e.g., 6faf1bbc-6e4a-4454-a507-a14ef8e1bc5c, etc. Default value = NA) • ocscp_service_instance_id (e.g., fe137ab7-740a-46ee-aa5c-951806d77b02, etc. Default value = NA)	• ocscp_metric_total_attempts_to_forward_route{ocscp_nf_type="UDM"} • ocscp_metric_total_attempts_to_forward_route{ocscp_nf_service_type="nudm-uecm"} • ocscp_metric_total_attempts_to_forward_route{ocscp_nf_end_point="10.96.166.65:80"} • ocscp_metric_total_attempts_to_forward_route{ocscp_locality="Loc7"} • ocscp_metric_total_attempts_to_forward_route{ocscp_nf_instance_id="6faf1bbc-6e4a-4454-a507-a14ef8e1bc5c"} • ocscp_metric_total_attempts_to_forward_route{ocscp_service_instance_id="fe137ab7-740a-46ee-aa5c-951806d77b02"}

Table 5-4 (Cont.) Metrics Reference

Prometheus Stat Metric Name	Metric Description	Dimensions	Example usage to filter metric by dimension on Grafana GUI
ocscp_metric_total_upstream_send_fail	Total number of request that SCP failed to send to the upstream cluster	• ocscp_nf_type (e.g., UDM, PCF, AMF, etc.) • ocscp_nf_service_type (e.g., nudm-uecm, nudm-sdm, etc.) • ocscp_nf_end_point (Default value = 0.0:00) • ocscp_locality (SCP site name e.g., Loc6, Loc7, etc.) • ocscp_nf_instance_id (e.g., 6faf1bbc-6e4a-4454-a507-a14ef8e1bc5c, etc. Default value = NA) • ocscp_service_instance_id (e.g., fe137ab7-740a-46ee-aa5c-951806d77b02, etc. Default value = NA)	• ocscp_metric_total_upstream_send_fail{ocscp_nf_type="UDM"} • ocscp_metric_total_upstream_send_fail{ocscp_nf_service_type="nudm-uecm"} • ocscp_metric_total_upstream_send_fail{ocscp_nf_end_point="10.96.166.65:80"} • ocscp_metric_total_upstream_send_fail{ocscp_locality="Loc7"} • ocscp_metric_total_upstream_send_fail{ocscp_nf_instance_id="6faf1bbc-6e4a-4454-a507-a14ef8e1bc5c"} • ocscp_metric_total_upstream_send_fail{ocscp_service_instance_id="fe137ab7-740a-46ee-aa5c-951806d77b02"}

Table 5-4 (Cont.) Metrics Reference

Prometheus Stat Metric Name	Metric Description	Dimensions	Example usage to filter metric by dimension on Grafana GUI
ocscp_metric_total_routing_send_fail	Total number of request that SCP failed to route due to any reason	• ocscp_nf_type (e.g., UDM, PCF, AMF, etc.) • ocscp_nf_service_type (e.g., nudm-uecm, nudm-sdm, etc.) • ocscp_nf_end_point (Default value = 0.0:00) • ocscp_locality (SCP site name e.g., Loc6, Loc7, etc.) • ocscp_nf_instance_id (e.g., 6faf1bbc-6e4a-4454-a507-a14ef8e1bc5c, etc. Default value = NA) • ocscp_service_instance_id (e.g., fe137ab7-740a-46ee-aa5c-951806d77b02, etc. Default value = NA)	• ocscp_metric_total_routing_send_fail{ocscp_nf_type="UDM"} • ocscp_metric_total_routing_send_fail{ocscp_nf_service_type="nudm-uecm"} • ocscp_metric_total_routing_send_fail{ocscp_nf_end_point="10.96.166.65:80"} • ocscp_metric_total_routing_send_fail{ocscp_locality="Loc7"} • ocscp_metric_total_routing_send_fail{ocscp_nf_instance_id="6faf1bbc-6e4a-4454-a507-a14ef8e1bc5c"} • ocscp_metric_total_routing_send_fail{ocscp_service_instance_id="fe137ab7-740a-46ee-aa5c-951806d77b02"}

Table 5-4 (Cont.) Metrics Reference

Prometheus Stat Metric Name	Metric Description	Dimensions	Example usage to filter metric by dimension on Grafana GUI
ocscp_metric_request_processing_time	This metric captures the processing time by SCP for ingress requests into the time buckets(e.g., 1ms, 2ms, 4ms, 8ms and so on)	• ocscp_nf_type (e.g., UDM, PCF, AMF, etc.) • ocscp_nf_service_type (e.g., nudm-uecm, nudm-sdm, etc.) • ocscp_nf_end_point (Default value = 0.0:00) • ocscp_locality (SCP site name e.g., Loc6, Loc7, etc.) • ocscp_nf_instance_id (e.g., 6faf1bbc-6e4a-4454-a507-a14ef8e1bc5c, etc. Default value = NA) • ocscp_service_instance_id (e.g., fe137ab7-740a-46ee-aa5c-951806d77b02, etc. Default value = NA) • ocscp_processing_time (e.g., 1ms, 2ms, 4ms, 8ms, etc.)	• ocscp_metric_request_processing_time{ocscp_nf_type="UDM"} • ocscp_metric_request_processing_time{ocscp_nf_service_type="nudm-uecm"} • ocscp_metric_request_processing_time{ocscp_nf_end_point="10.96.166.65:80"} • ocscp_metric_request_processing_time{ocscp_locality="Loc7"} • ocscp_metric_request_processing_time{ocscp_nf_instance_id="6faf1bbc-6e4a-4454-a507-a14ef8e1bc5c"} • ocscp_metric_request_processing_time{ocscp_service_instance_id="fe137ab7-740a-46ee-aa5c-951806d77b02"} • ocscp_metric_request_processing_time{ocscp_processing_time="1ms"}

Table 5-4 (Cont.) Metrics Reference

Prometheus Stat Metric Name	Metric Description	Dimensions	Example usage to filter metric by dimension on Grafana GUI
ocscp_metric_response_processing_time	This metric captures the processing time by SCP for ingress responses into the time buckets(e.g., 1ms, 2ms, 4ms, 8ms and so on)	• ocscp_nf_type (e.g., UDM, PCF, AMF, etc.) • ocscp_nf_service_type (e.g., nudm-uecm, nudm-sdm, etc.) • ocscp_nf_end_point (Default value = 0.0:00) • ocscp_locality (SCP site name e.g., Loc6, Loc7, etc.) • ocscp_nf_instance_id (e.g., 6faf1bbc-6e4a-4454-a507-a14ef8e1bc5c, etc. Default value = NA) • ocscp_service_instance_id (e.g., fe137ab7-740a-46ee-aa5c-951806d77b02, etc. Default value = NA) • ocscp_processing_time (e.g., 1ms, 2ms, 4ms, 8ms, etc.)	• ocscp_metric_response_processing_time{ocscp_nf_type="UDM"} • ocscp_metric_response_processing_time{ocscp_nf_service_type="nudm-uecm"} • ocscp_metric_response_processing_time{ocscp_nf_end_point="10.96.166.65:80"} • ocscp_metric_response_processing_time{ocscp_locality="Loc7"} • ocscp_metric_response_processing_time{ocscp_nf_instance_id="6faf1bbc-6e4a-4454-a507-a14ef8e1bc5c"} • ocscp_metric_response_processing_time{ocscp_service_instance_id="fe137ab7-740a-46ee-aa5c-951806d77b02"} • ocscp_metric_response_processing_time{ocscp_processing_time="1ms"}

Table 5-4 (Cont.) Metrics Reference

Prometheus Stat Metric Name	Metric Description	Dimensions	Example usage to filter metric by dimension on Grafana GUI
ocscp_metric_request_per_try_timeout	This metric captures the number of incoming request whose per try timeout expired	• ocscp_nf_type (e.g., UDM, PCF, AMF, etc.) • ocscp_nf_service_type (e.g., nudm-uecm, nudm-sdm, etc.) • ocscp_nf_end_point (Default value = 0.0:00) • ocscp_locality (SCP site name e.g., Loc6, Loc7, etc.) • ocscp_nf_instance_id (e.g., 6faf1bbc-6e4a-4454-a507-a14ef8e1bc5c, etc. Default value = NA) • ocscp_service_instance_id (e.g., fe137ab7-740a-46ee-aa5c-951806d77b02, etc. Default value = NA)	• ocscp_metric_request_per_try_timeout{ocscp_nf_type="UDM"} • ocscp_metric_request_per_try_timeout{ocscp_nf_service_type="nudm-uecm"} • ocscp_metric_request_per_try_timeout{ocscp_nf_end_point="10.96.166.65:80"} • ocscp_metric_request_per_try_timeout{ocscp_locality="Loc7"} • ocscp_metric_request_per_try_timeout{ocscp_nf_instance_id="6faf1bbc-6e4a-4454-a507-a14ef8e1bc5c"} • ocscp_metric_request_per_try_timeout{ocscp_service_instance_id="fe137ab7-740a-46ee-aa5c-951806d77b02"}

Table 5-4 (Cont.) Metrics Reference

Prometheus Stat Metric Name	Metric Description	Dimensions	Example usage to filter metric by dimension on Grafana GUI
ocscp_metric_total_transaction_timeout	This metric captures the total number of request whose transaction timed out	• ocscp_nf_type (e.g., UDM, PCF, AMF, etc.) • ocscp_nf_service_type (e.g., nudm-uecm, nudm-sdm, etc.) • ocscp_nf_end_point (Default value = 0.0:00) • ocscp_locality (SCP site name e.g., Loc6, Loc7, etc.) • ocscp_nf_instance_id (e.g., 6faf1bbc-6e4a-4454-a507-a14ef8e1bc5c, etc. Default value = NA) • ocscp_service_instance_id (e.g., fe137ab7-740a-46ee-aa5c-951806d77b02, etc. Default value = NA)	• ocscp_metric_total_transaction_timeout{ocscp_nf_type="UDM"} • ocscp_metric_total_transaction_timeout{ocscp_nf_service_type="nudm-uecm"} • ocscp_metric_total_transaction_timeout{ocscp_nf_end_point="10.96.166.65:80"} • ocscp_metric_total_transaction_timeout{ocscp_locality="Loc7"} • ocscp_metric_total_transaction_timeout{ocscp_nf_instance_id="6faf1bbc-6e4a-4454-a507-a14ef8e1bc5c"} • ocscp_metric_total_transaction_timeout{ocscp_service_instance_id="fe137ab7-740a-46ee-aa5c-951806d77b02"}

Table 5-4 (Cont.) Metrics Reference

Prometheus Stat Metric Name	Metric Description	Dimensions	Example usage to filter metric by dimension on Grafana GUI
ocscp_metric_max_routing_attempts_exhausted	This metric captures the total number of requests whose maximum routing attempts expired during alternate routing	• ocscp_nf_type (e.g., UDM, PCF, AMF, etc.) • ocscp_nf_service_type (e.g., nudm-uecm, nudm-sdm, etc.) • ocscp_nf_end_point (Default value = 0.0:00) • ocscp_locality (SCP site name e.g., Loc6, Loc7, etc.) • ocscp_nf_instance_id (e.g., 6faf1bbc-6e4a-4454-a507-a14ef8e1bc5c, etc. Default value = NA) • ocscp_service_instance_id (e.g., fe137ab7-740a-46ee-aa5c-951806d77b02, etc. Default value = NA)	• ocscp_metric_max_routing_attempts_exhausted{ocscp_nf_type="UDM"} • ocscp_metric_max_routing_attempts_exhausted{ocscp_nf_service_type="nudm-uecm"} • ocscp_metric_max_routing_attempts_exhausted{ocscp_nf_end_point="10.96.166.65:80"} • ocscp_metric_max_routing_attempts_exhausted{ocscp_locality="Loc7"} • ocscp_metric_max_routing_attempts_exhausted{ocscp_nf_instance_id="6faf1bbc-6e4a-4454-a507-a14ef8e1bc5c"} • ocscp_metric_max_routing_attempts_exhausted{ocscp_service_instance_id="fe137ab7-740a-46ee-aa5c-951806d77b02"}

Table 5-4 (Cont.) Metrics Reference

Prometheus Stat Metric Name	Metric Description	Dimensions	Example usage to filter metric by dimension on Grafana GUI
ocscp_sds_dbmetrics_total	Total number of db operations (create, update, delete and find) Metrics Pegging Condition: This metrics is pegged whenever create, update, delete and find operation are triggered.	1. nftype (eg: amf,smf) 2. ueid 3. dboperation 4. responsecode 5. tablename	**AMF CREATE SUCCESS** • ocscp_sds_dbmetrics_total{nftype="amf",dboperation="create",responsecode="200",table="subscriberamfbindingdata",ueid="supi;gpsi;pei"} • ocscp_sds_dbmetrics_total{nftype="amf",dboperation="create",responsecode="200",table="subscriberamfbindinggpsi",ueid="supi;gpsi"} • ocscp_sds_dbmetrics_total{nftype="amf",dboperation="create",responsecode="200",table="subscriberamfbindingpei",ueid="supi;pei"} **AMF CREATE FAILURE** • ocscp_sds_dbmetrics_total{nftype="amf",dboperation="create",responsecode="400",table="unknown",ueid="unknown"} • ocscp_sds_dbmetrics_total{nftype="amf",dboperation="create",responsecode="422",table="unknown",ueid="unknown"} • ocscp_sds_dbmetrics_total{nftype="amf",dboperation="create",responsecode="500",table="unknown",ueid="unknown"} **AMF UPDATE SUCCESS** • ocscp_sds_dbmetrics_total{nftype="amf",dboperation="update",responsecode="200",table="subscriberamfbindingdata",ueid="supi;gpsi;pei"} • ocscp_sds_dbmetrics_total{nftype="amf",dboperation="update",responsecode="200",table="subscriberamfbindinggpsi",ueid="supi;gpsi"} • ocscp_sds_dbmetrics_total{nftype="amf",dboperation="update",responsecode="200",table="subscriberamfbindingpei",ueid="supi;pei"}

Table 5-4 (Cont.) Metrics Reference

Prometheus Stat Metric Name	Metric Description	Dimensions	Example usage to filter metric by dimension on Grafana GUI
			AMF UPDATE FAILURE • ocscp_sds_dbmetrics_total{nftype="amf",dboperation="update",responsecode="400",table="subscriberamfbindingdata",ueid="supi;gpsi;pei"} • ocscp_sds_dbmetrics_total{nftype="amf",dboperation="update",responsecode="400",table="unknown",ueid="unknown"} • ocscp_sds_dbmetrics_total{nftype="amf",dboperation="update",responsecode="500",table="unknown",ueid="unknown"} **AMF FIND SUCCESS** • ocscp_sds_dbmetrics_total{nftype="amf",dboperation="find",responsecode="200",table="subscriberamfbindingdata",ueid="supi"} • ocscp_sds_dbmetrics_total{nftype="amf",dboperation="find",responsecode="200",table="subscriberamfbindingdata",ueid="supi;amfinstanceid} • ocscp_sds_dbmetrics_total{nftype="amf",dboperation="find",responsecode="200",table="subscriberamfbindingdata",ueid="supi;gpsi} • ocscp_sds_dbmetrics_total{nftype="amf",dboperation="find",responsecode="200",table="subscriberamfbindingdata",ueid="supi;guami} • ocscp_sds_dbmetrics_total{nftype="amf",dboperation="find",responsecode="200",table="subscriberamfbindingdata",ueid="supi;groupid} • ocscp_sds_dbmetrics_total{nftype="amf",dboperation="find",responsecode="200",table="subscriberamfbindingdata",ueid="supi;pei} • ocscp_sds_dbmetrics_total{nftype="amf",dboperation

Table 5-4 (Cont.) Metrics Reference

Prometheus Stat Metric Name	Metric Description	Dimensions	Example usage to filter metric by dimension on Grafana GUI
			="find",responsecode="200",table="subscriberamfbindingdata,subscriberamfbindinggpsi",ueid="gpsi"} • ocscp_sds_dbmetrics_total{nftype="amf",dboperation="find",responsecode="200",table="subscriberamfbindingdata,subscriberamfbindingpei",ueid="pei"} **AMF FIND FAILURE** • ocscp_sds_dbmetrics_total{nftype="amf",dboperation="find",responsecode="400",table="subscriberamfbindingdata",ueid="invalidparam"} • ocscp_sds_dbmetrics_total{nftype="amf",dboperation="find",responsecode="404",table="subscriberamfbindingdata",ueid="supi"} • ocscp_sds_dbmetrics_total{nftype="amf",dboperation="find",responsecode="404",table="subscriberamfbindingdata",ueid="supi;amfinstanceid} • ocscp_sds_dbmetrics_total{nftype="amf",dboperation="find",responsecode="404",table="subscriberamfbindingdata",ueid="supi;gpsi} • ocscp_sds_dbmetrics_total{nftype="amf",dboperation="find",responsecode="404",table="subscriberamfbindingdata",ueid="supi;guami} • ocscp_sds_dbmetrics_total{nftype="amf",dboperation="find",responsecode="404",table="subscriberamfbindingdata",ueid="supi;groupid} • ocscp_sds_dbmetrics_total{nftype="amf",dboperation="find",responsecode="404",table="subscriberamfbindingdata",ueid="supi;pei} • ocscp_sds_dbmetrics_total{nftype="amf",dboperation="find",responsecode="404

Table 5-4 (Cont.) Metrics Reference

Prometheus Stat Metric Name	Metric Description	Dimensions	Example usage to filter metric by dimension on Grafana GUI
			",table="subscriberamfbindingdata;subscriberamfbindinggpsi",ueid="gpsi"} • ocscp_sds_dbmetrics_total{nftype="amf",dboperation="find",responsecode="404",table="subscriberamfbindingdata;subscriberamfbindingpei",ueid="pei"} • ocscp_sds_dbmetrics_total{nftype="amf",dboperation="find",responsecode="500",table="unknown",ueid="unknown"} **AMF DELETE SUCCESS** • ocscp_sds_dbmetrics_total{nftype="amf",dboperation="delete",responsecode="200",table="subscriberamfbindingdata",ueid="supi;gpsi"} • ocscp_sds_dbmetrics_total{nftype="amf",dboperation="delete",responsecode="200",table="subscriberamfbindingdata",ueid="supi;guami"} • ocscp_sds_dbmetrics_total{nftype="amf",dboperation="delete",responsecode="200",table="subscriberamfbindingdata",ueid="supi;amfinstanceid"} • ocscp_sds_dbmetrics_total{nftype="amf",dboperation="delete",responsecode="200",table="subscriberamfbindingdata",ueid="supi;groupid"} • ocscp_sds_dbmetrics_total{nftype="amf",dboperation="delete",responsecode="200",table="subscriberamfbindingdata",ueid="supi;pei"} • ocscp_sds_dbmetrics_total{nftype="amf",dboperation="delete",responsecode="200",table="subscriberamfbindinggpsi",ueid="supi;gpsi"} • ocscp_sds_dbmetrics_total{nftype="amf",dboperation

Table 5-4 (Cont.) Metrics Reference

Prometheus Stat Metric Name	Metric Description	Dimensions	Example usage to filter metric by dimension on Grafana GUI
			="delete",responsecode="200",table="subscriberamfbindingpei",ueid="supi;pei"} **AMF DELETE FAILURE** • ocscp_sds_dbmetrics_total{nftype="amf",dboperation="delete",responsecode="500",table="subscriberamfbindingdata",ueid="unknown"} **AMF UNKNOWN FAILURE** • ocscp_sds_dbmetrics_total{nftype="amf",dboperation="unknown",responsecode="500",table="unknown",ueid="unknown"} **SMF CREATE SUCCESS** • ocscp_sds_dbmetrics_total{nftype="smf",dboperation="create",responsecode="200",table="subscribersmfbindingdata",ueid="supi;pdussessionid"} **SMF CREATE FAILURE** • ocscp_sds_dbmetrics_total{nftype="smf",dboperation="create",responsecode="400",table="subscribersmfbindingdata",ueid="supi;pdussessionid"} • ocscp_sds_dbmetrics_total{nftype="smf",dboperation="create",responsecode="422",table="subscribersmfbindingdata",ueid="supi;pdussessionid"} • ocscp_sds_dbmetrics_total{nftype="smf",dboperation="create",responsecode="500",table="subscribersmfbindingdata",ueid="supi;pdussessionid"} **SMF UPDATE SUCCESS** • ocscp_sds_dbmetrics_total{nftype="smf",dboperation="update",responsecode="200",table="subscribersmfbindingdata",ueid="supi;pdusessionid"} **SMF UPDATE FAILURE** • ocscp_sds_dbmetrics_total{nftype="smf",dboperation

Table 5-4 (Cont.) Metrics Reference

Prometheus Stat Metric Name	Metric Description	Dimensions	Example usage to filter metric by dimension on Grafana GUI
			="update",responsecode="400",table="subscribersmfbindingdata",ueid="supi;pdusessionid"} • ocscp_sds_dbmetrics_total{nftype="smf",dboperation="update",responsecode="500",table="subscribersmfbindingdata",ueid="supi;pdusessionid"} **SMF DELETE SUCCESS** • ocscp_sds_dbmetrics_total{nftype="smf",dboperation="delete",responsecode="200",table="subscribersmfbindingdata",ueid="supi;pdusessionid"} **SMF DELETE FAILURE** • ocscp_sds_dbmetrics_total{nftype="smf",dboperation="delete",responsecode="400",table="subscribersmfbindingdata",ueid="invalidparam"} • ocscp_sds_dbmetrics_total{nftype="smf",dboperation="delete",responsecode="500",table="subscribersmfbindingdata",ueid="supi;pdusessionid"} **SMF FIND SUCCESS** • ocscp_sds_dbmetrics_total{nftype="smf",dboperation="find",responsecode="200",table="subscribersmfbindingdata",ueid="supi;pdusessionid"} • ocscp_sds_dbmetrics_total{nftype="smf",dboperation="find",responsecode="200",table="subscribersmfbindingdata",ueid="gpsi;pdusessionid"} **SMF FIND FAILURE** • ocscp_sds_dbmetrics_total{nftype="smf",dboperation="find",responsecode="400",table="subscribersmfbindingdata",ueid="invalidparam"} • ocscp_sds_dbmetrics_total{nftype="smf",dboperation

Table 5-4 (Cont.) Metrics Reference

Prometheus Stat Metric Name	Metric Description	Dimensions	Example usage to filter metric by dimension on Grafana GUI
			="find",responsecode="404",table="subscribersmfbindingdata",ueid="supi;pdusessionid"} • ocscp_sds_dbmetrics_total{nftype="smf",dboperation="find",responsecode="404",table="subscribersmfbindingdata",ueid="gpsi;pdusessionid"} • ocscp_sds_dbmetrics_total{nftype="smf",dboperation="find",responsecode="500",table="subscribersmfbindingdata",ueid="unknown"} **SMF UNKNOWN FAILURE** • ocscp_sds_dbmetrics_total{nftype="smf",dboperation="unknown",responsecode="500",table="unknown",ueid="unknown"}

Table 5-4 (Cont.) Metrics Reference

Prometheus Stat Metric Name	Metric Description	Dimensions	Example usage to filter metric by dimension on Grafana GUI
ocscp_sds_dbmetrics_latencies_seconds_bucket	Calculates processing time of each database request and put those values in a seconds bucket. Seconds bucket configured with [0.1,0.2,0.4,0.8,1.0,2.0,4.0,8.0,10.0] values.	1. nftype (eg: amf,smf) 2. ueid 3. dboperation 4. le (time in millisecond) 5. tablename	• ocscp_sds_dbmetrics_total{nftype="amf",dboperation="create",table="subscriberamfbindingdata",ueid="supi;gpsi;pei"} • ocscp_sds_dbmetrics_total{nftype="amf",dboperation="create",table="subscriberamfbindinggpsi",ueid="supi;gpsi"} • ocscp_sds_dbmetrics_total{nftype="amf",dboperation="create",table="subscriberamfbindingpei",ueid="supi;pei"} • ocscp_sds_dbmetrics_total{nftype="amf",dboperation="update",table="subscriberamfbindingdata",ueid="supi;gpsi;pei"} • ocscp_sds_dbmetrics_total{nftype="amf",dboperation="update",table="subscriberamfbindinggpsi",ueid="supi;gpsi"} • ocscp_sds_dbmetrics_total{nftype="amf",dboperation="update",table="subscriberamfbindingpei",ueid="supi;pei"} • ocscp_sds_dbmetrics_total{nftype="amf",dboperation="find",table="subscriberamfbindingdata",ueid="supi"} • ocscp_sds_dbmetrics_total{nftype="amf",dboperation="find",table="subscriberamfbindingdata",ueid="supi;amfinstanceid} • ocscp_sds_dbmetrics_total{nftype="amf",dboperation="find",table="subscriberamfbindingdata",ueid="supi;gpsi} • ocscp_sds_dbmetrics_total{nftype="amf",dboperation="find",table="subscriberamfbindingdata",ueid="supi;groupid} • ocscp_sds_dbmetrics_total{nftype="amf",dboperation="find",table="subscribera

Table 5-4 (Cont.) Metrics Reference

Prometheus Stat Metric Name	Metric Description	Dimensions	Example usage to filter metric by dimension on Grafana GUI
			mfbindingdata",ueid="supi;pei} • ocscp_sds_dbmetrics_total{nftype="amf",dboperation="find",table="subscriberamfbindingdata,subscriberamfbindinggpsi",ueid="gpsi"} • ocscp_sds_dbmetrics_total{nftype="amf",dboperation="find",table="subscriberamfbindingdata,subscriberamfbindingpei",ueid="pei"} • ocscp_sds_dbmetrics_total{nftype="amf",dboperation="find",table="subscriberamfbindingdata",ueid="supi"} • ocscp_sds_dbmetrics_total{nftype="amf",dboperation="find",table="subscriberamfbindingdata",ueid="supi;amfinstanceid} • ocscp_sds_dbmetrics_total{nftype="amf",dboperation="find",table="subscriberamfbindingdata",ueid="supi;gpsi} • ocscp_sds_dbmetrics_total{nftype="amf",dboperation="find",table="subscriberamfbindingdata",ueid="supi;guami} • ocscp_sds_dbmetrics_total{nftype="amf",dboperation="find",table="subscriberamfbindingdata",ueid="supi;groupid} • ocscp_sds_dbmetrics_total{nftype="amf",dboperation="find",table="subscriberamfbindingdata",ueid="supi;pei} • ocscp_sds_dbmetrics_total{nftype="amf",dboperation="find",table="subscriberamfbindingdata,subscriberamfbindinggpsi",ueid="gpsi"} • ocscp_sds_dbmetrics_total{nftype="amf",dboperation="find",table="subscriberamfbindingdata,subscriberamfbindingpei",ueid="pei"} • ocscp_sds_dbmetrics_total{nftype="smf",dboperation

Table 5-4 (Cont.) Metrics Reference

Prometheus Stat Metric Name	Metric Description	Dimensions	Example usage to filter metric by dimension on Grafana GUI
			="create",table="subscribersmfbindingdata",ueid="supi;pdusessionid"} • ocscp_sds_dbmetrics_total{nftype="smf",dboperation="update",table="subscribersmfbindingdata",ueid="supi;pdusessionid"} • ocscp_sds_dbmetrics_total{nftype="smf",dboperation="delete",table="subscribersmfbindingdata",ueid="supi;pdusessionid"} • ocscp_sds_dbmetrics_total{nftype="smf",dboperation="find",table="subscribersmfbindingdata",ueid="supi;pdusessionid"} • ocscp_sds_dbmetrics_total{nftype="smf",dboperation="find",table="subscribersmfbindingdata",ueid="gpsi;pdusessionid"}
hosts_cx_total	Total number of connections attempted to the host Metrics Pegging Condition: New connection attempted.	1. cluster_name 2. endpoint	hosts_cx_total{cluster_name="outbound|80||udm1_udm1svc_svc_cluster_local",endpoint="192.168.219.75:80"}
hosts_cx_active	Total number of active connections to the host Metrics Pegging Condition: New connection established and active (no failure or disconnect).	1. cluster_name 2. endpoint	hosts_cx_active{cluster_name="outbound|80||udm1_udm1svc_svc_cluster_local",endpoint="192.168.219.75:80"}

Table 5-4 (Cont.) Metrics Reference

Prometheus Stat Metric Name	Metric Description	Dimensions	Example usage to filter metric by dimension on Grafana GUI
hosts_cx_connect_fail	Total number of connection attempts to the host which resulted in failure (local + remote failures) Metrics Pegging Condition: Connection attempt failed.	1. cluster_name 2. endpoint	hosts_cx_connect_fail{cluster_name="outbound|80|| udm1_udm1svc_svc_cluster_local",endpoint="192.168.219.75:80"}
hosts_rq_total	Total requests sent to the host Metrics Pegging Condition: Request forwarded to host.	1. cluster_name 2. endpoint	hosts_rq_total{cluster_name="outbound|80|| udm1_udm1svc_svc_cluster_local",endpoint="192.168.219.75:80"}
hosts_rq_timeout	Total timed out requests Metrics Pegging Condition: Request timed out (upon expiry of timeout).	1. cluster_name 2. endpoint	hosts_rq_timeout{cluster_name="outbound|80|| udm1_udm1svc_svc_cluster_local",endpoint="192.168.219.75:80"}
hosts_rq_success	Total requests with non-5xx responses from host Metrics Pegging Condition: Success(non 5xx) response received from host.	1. cluster_name 2. endpoint	hosts_rq_success{cluster_name="outbound|80|| udm1_udm1svc_svc_cluster_local",endpoint="192.168.219.75:80"}
hosts_rq_error	Total requests with 5xx responses from host Metrics Pegging Condition: Failure(5xx) response received from host.	1. cluster_name 2. endpoint	hosts_rq_error{cluster_name="outbound|80|| udm1_udm1svc_svc_cluster_local",endpoint="192.168.219.75:80"}

Table 5-4 (Cont.) Metrics Reference

Prometheus Stat Metric Name	Metric Description	Dimensions	Example usage to filter metric by dimension on Grafana GUI
hosts_rq_active	Total active requests (in-flight transactions) Metrics Pegging Condition: Request forwarded to host. It is decremented once response is received.	1. cluster_name 2. endpoint	hosts_rq_active{cluster_name="outbound|80|| udm1_udm1svc_svc_cluster_local",endpoint="192.168.219.75:80"}
hosts_success_rate	Request success rate (0-100). If there was not enough request volume in the interval to calculate it.	1. cluster_name 2. endpoint	hosts_success_rate{cluster_name="outbound|80|| udm1_udm1svc_svc_cluster_local",endpoint="192.168.219.75:80"}
scp_notifications_rejected_topologysource_local_total	Number of NF notification messages rejected because "learning from NRF" was configured as "not allowed". Metrics Pegging Condition: This metrics will be pegged whenever notification is received for NF configured as LOCAL.	nftype (eg: UDM, AMF)	scp_local_topology_source_total{NFType = "UDM"}
scp_topologysource_toggle_nrf_to_local_total	Number of times topology source changed from "NRF" to "Local" for given NF.	nftype (eg: UDM, AMF)	scp_topologysource_toggle_nrf_to_local_total{NFType = "UDM"}
scp_topologysource_toggle_local_to_nrf_total	Number of times topology source changed from "Local" to "NRF" for given NF.	nftype (eg: UDM, AMF)	scp_topologysource_toggle_local_to_nrf_total{NFType = "UDM"}
scp_soothsayer_audit_db_fetch_failure_total	Number of times audit failed due to database failure		scp_soothsayer_audit_db_fetch_failure

Table 5-4 (Cont.) Metrics Reference

Prometheus Stat Metric Name	Metric Description	Dimensions	Example usage to filter metric by dimension on Grafana GUI
scp_soothsayer_subscription_db_fetch_failure_total	Number of times subscription failed due to database failure		scp_soothsayer_subscription_db_fetch_failure
scp_failure_processed_nf_notification_total	Number of times notification process failure	1. nftype (eg., AMF) 2. nfInstanceId	scp_failure_processed_nf_notification{nftype="UDM",nfinstanceid="6faf3abc-6e4a-4454-a507-a14ef8e1bc4b"}
ocscp_metric_total_app_req	Number of request for ocscp_app (mediation and amf/smf db messages) at scp-worker This metric can be used in conjunction with 'ocscp_metric_total_http_rx_req' to calculate percentage of message processing by mediation.	1. ocscp_app_name (nmediation_http, ocscp-sds-amf and ocscp-sds-smf) 2. ocscp_trigger_name (OnRequestIngress, OnRequestEgress, OnResponseIngress, OnResponseEgress) 3. ocscp_nf_type (e.g., UDM, PCF, AMF, etc.) 4. ocscp_nf_service_type (e.g., nudm-uecm, nudm-sdm, etc.) 5. ocscp_nf_end_point (Default value = 0.0:00)	ocscp_metric_total_app_req{ocscp_app_name="ocscp-sds-amf"} ocscp_metric_total_app_req{ocscp_trigger_name="OnRequestIngress"} ocscp_metric_total_app_req{ocscp_nf_type="UDM"} ocscp_metric_total_app_req{ocscp_nf_service_type="nudm-uecm"} ocscp_metric_total_app_req{ocscp_nf_end_point="10.96.166.65:80"} ocscp_metric_total_app_req{ocscp_locality="Loc7"} ocscp_metric_total_app_req{ocscp_nf_instance_id="6faf1bbc-6e4a-4454-a507-a14ef8e1bc5c"} ocscp_metric_total_app_req{ocscp_service_instance_id="fe137ab7-740a-46ee-aa5c-951806d77b02"}

Table 5-4 (Cont.) Metrics Reference

Prometheus Stat Metric Name	Metric Description	Dimensions	Example usage to filter metric by dimension on Grafana GUI
ocscp_metric_total_app_res	Number of response for ocscp_app (mediation and amf/smf db messages) at scp-worker	1. ocscp_app_name (nmediation_http, ocscp-sds-amf and ocscp-sds-smf) 2. ocscp_trigger_name (OnRequestIngress, OnRequestEgress, OnResponseIngress, OnResponseEgress) 3. ocscp_msg_size (The response message size buckets. e.g., 1K (size < 1k bytes), 2K (1k < size < 2k bytes), 4K (2k < size < 4k), etc.)) 4. ocscp_response_code (e.g. 200, 201, etc.) 5. ocscp_nf_type (e.g., UDM, PCF, AMF, etc.) 6. ocscp_nf_service_type (e.g., nudm-uecm, nudm-sdm, etc.) 7. ocscp_nf_end_point (Default value = 0.0:00) 8. ocscp_locality (SCP site name e.g., Loc6, Loc7, etc.) 9. ocscp_nf_instance_id (e.g., 6faf1bbc-6e4a-4454-a507-a14ef8e1bc5c,	ocscp_metric_total_app_req{ocscp_app_name="ocscp-sds-amf"} ocscp_metric_total_app_req{ocscp_trigger_name="OnRequestIngress"} ocscp_metric_total_app_req{ocscp_nf_type="UDM"} ocscp_metric_total_app_req{ocscp_nf_service_type="nudm-uecm"} ocscp_metric_total_app_req{ocscp_nf_end_point="10.96.166.65:80"} ocscp_metric_total_app_req{ocscp_locality="Loc7"} ocscp_metric_total_app_req{ocscp_nf_instance_id="6faf1bbc-6e4a-4454-a507-a14ef8e1bc5c"} ocscp_metric_total_app_req{ocscp_service_instance_id="fe137ab7-740a-46ee-aa5c-951806d77b02"} **Note**: Dimension "ocscp_trigger_name" and "ocscp_msg_size " cannot be used together.

Table 5-4 (Cont.) Metrics Reference

Prometheus Stat Metric Name	Metric Description	Dimensions	Example usage to filter metric by dimension on Grafana GUI
		etc. Default value = NA) 10. ocscp_service_instance_id (e.g., fe137ab7-740a-46ee-aa5c-951806d77b02, etc. Default value = NA)	
ocscp_http_downstream_cx_destroy_remote_active_rq	Number of downstream connections destroyed from remote end with active requests i.e. SCP was still processing the request from the downstream peer.	*ocscp_http_conn_manager_prefix* - Stat prefix for the listener. If not specified it is constructed using listener address. For example, 0.0.0.0_8080 for SCP signaling port.	ocscp_http_downstream_cx_destroy_remote_active_rq{ocscp_http_conn_manager_prefix="0.0.0.0_8080"} **Note**: This metric is usually accompanied by a warning log to show downstream peer address.
scp_patch_subscription_nf_success_total	Number of successful patch operation of subscription based on nfType and ServingScope	1. nftype (eg: UDM, AMF) 2. ServingScope (eg: Reg1,Reg2)	scp_patch_subscription_nf_success_total{nftype="AUSF",ServingScope="Reg1"}
scp_patch_subscription_nf_failure_total	Number of failure patch operation of subscription based on nfType and ServingScope	1. nftype (eg: UDM, AMF) 2. ServingScope (eg: Reg1,Reg2)	scp_patch_subscription_nf_failure_total{nftype="AUSF",ServingScope="Reg1"}
scp_unsubscription_nf_success_total	Number of successful operations of unsubscription based on nftype and servingscope	1. nftype (eg: UDM, AMF) 2. ServingScope (eg: Reg1,Reg2)	scp_unsubscription_nf_success_total{nftype="AUSF",ServingScope="Reg1"}
scp_unsubscription_nf_failure_total	Number of successful operations of unsubscription based on nftype and servingscope	1. nftype (eg: UDM, AMF) 2. ServingScope (eg:Reg1,Reg2)	scp_unsubscription_nf_failure_total{nftype="AUSF",ServingScope="Reg1"}

Table 5-4 (Cont.) Metrics Reference

Prometheus Stat Metric Name	Metric Description	Dimensions	Example usage to filter metric by dimension on Grafana GUI
scp_subscription_nf_success_total	Number of successful operations of subscription based on nftype and servingscope	1. nftype (eg: UDM, AMF) 2. ServingScope (eg:Reg1,Reg2)	scp_subscription_nf_success_total{nftype="AUSF",ServingScope="Reg1"}
scp_subscription_nf_failure_total	Number of successful operations of subscription based on nftype and servingscope	1. nftype (eg: UDM, AMF) 2. ServingScope (eg:Reg1,Reg2)	scp_subscription_nf_failure_total{nftype="AUSF",ServingScope="Reg1"}
scp_soothsayer_audit_2xx_empty_nf_array	The state of metrics will be 1 when scp audit receives empty nf array response for nftype. Then state of metrics will be change to 0 when audit receives non empty nf array.		scp.soothsayer_audit_2xx_empty_nf_array{}
scp_soothsayer_audit_error_response	The state of metrics will be 1 when scp audit receives error response for nftype. Then state of metrics will be change to 0 when audit receives non error response for nftype.		scp.soothsayer_audit_error_response{}

Table 5-4 (Cont.) Metrics Reference

Prometheus Stat Metric Name	Metric Description	Dimensions	Example usage to filter metric by dimension on Grafana GUI
scp_soothsayer_db_operation_success_total	Number of successful soothsayer db Operations	1. dbOperation (eg: insert, getAll, insertOrUpdate, delete) 2. tablename (eg: NF_SUBSCRIPTIONS, NRF_NF_DETAILS)	scp_soothsayer_db_operation_success_total{dbOperation="insertOrUpdate",tableName="NF_SUBSCRIPTIONS"} scp_soothsayer_db_operation_success_total{dbOperation="getAll",tableName="NF_SUBSCRIPTIONS"} scp_soothsayer_db_operation_success_total{dbOperation="get",tableName="NF_SUBSCRIPTIONS"} scp_soothsayer_db_operation_success_total{dbOperation="delete",tableName="NF_SUBSCRIPTIONS"} scp_soothsayer_db_operation_success_total{dbOperation="insert",tableName="NRF_NF_DETAILS"} scp_soothsayer_db_operation_success_total{dbOperation="getAll",tableName="NRF_NF_DETAILS"}
scp_soothsayer_db_operation_failure_total	Number of failure soothsayer db Operations	1. dbOperation (eg: insert, getAll, insertOrUpdate, delete) 2. tablename (eg: NF_SUBSCRIPTIONS, NRF_NF_DETAILS)	scp_soothsayer_db_operation_failure_total{dbOperation="insertOrUpdate",tableName="NF_SUBSCRIPTIONS"} scp_soothsayer_db_operation_failure_total{dbOperation="getAll",tableName="NF_SUBSCRIPTIONS"} scp_soothsayer_db_operation_failure_total{dbOperation="get",tableName="NF_SUBSCRIPTIONS"} scp_soothsayer_db_operation_failure_total{dbOperation="delete",tableName="NF_SUBSCRIPTIONS"} scp_soothsayer_db_operation_failure_total{dbOperation="insert",tableName="NRF_NF_DETAILS"} scp_soothsayer_db_operation_failure_total{dbOperation="getAll",tableName="NRF_NF_DETAILS"}

Table 5-4 (Cont.) Metrics Reference

Prometheus Stat Metric Name	Metric Description	Dimensions	Example usage to filter metric by dimension on Grafana GUI
scp_soothsayer_nrf_registration_success_total	This metrics pegs the number of times registration successful for a particular serving scope.	servingScope ex: (Reg11,Reg1,Reg2)	scp_soothsayer_nrf_registration_success_total{servingScope="Reg11"}
scp_soothsayer_nrf_registration_failure_total	This metrics pegs the number of times registration failed for a particular serving scope.	servingScope ex: (Reg11,Reg1,Reg2)	scp_soothsayer_nrf_registration_failure_total{servingScope="Reg11"}
scp_soothsayer_nrf_heartbeat_success_total	This metrics pegs the number of times heartbeat successful for a particular serving scope.	servingScope ex: (Reg11,Reg1,Reg2)	scp_soothsayer_nrf_heartbeat_success_total{servingScope="Reg11"}
scp_soothsayer_nrf_heartbeat_failures_total	This metrics pegs the number of times heartbeat failed for a particular serving scope.	servingScope ex: (Reg11,Reg1,Reg2)	scp_soothsayer_nrf_heartbeat_failures_total{servingScope="Reg11"}
scp_soothsayer_mediation_total_rules_per_trigger	Total number of mediation rules configured per trigger point. To get cumulative value of all rules on all trigger, use the SUM function.	nftype nfservice trigger	

Table 5-4 (Cont.) Metrics Reference

Prometheus Stat Metric Name	Metric Description	Dimensions	Example usage to filter metric by dimension on Grafana GUI
ocscp_metric_upstream_service_time	This metric captures the time taken by upstream host is responding the request in time buckets (e.g., 1ms, 2ms, 4ms, 8ms and so on).	ocscp_nf_type (e.g., UDM, PCF, AMF, etc.) ocscp_nf_service_type (e.g., nudm-uecm, nudm-sdm, etc.) ocscp_nf_end_point (Default value = 0.0:00) ocscp_locality (SCP site name e.g., Loc6, Loc7, etc.) ocscp_nf_instance_id (e.g., 6faf1bbc-6e4a-4454-a507-a14ef8e1bc5c, etc. Default value = NA) ocscp_service_instance_id (e.g., fe137ab7-740a-46ee-aa5c-951806d77b02, etc. Default value = NA) ocscp_upstream_service_time (e.g., 1ms, 2ms, 4ms, 8ms, etc.)	ocscp_metric_upstream_service_time{ocscp_nf_type="UDM"} ocscp_metric_upstream_service_time{ocscp_nf_service_type="nudm-uecm"} ocscp_metric_upstream_service_time{ocscp_nf_end_point="10.96.166.65:80"} ocscp_metric_upstream_service_time{ocscp_locality="Loc7"} ocscp_metric_upstream_service_time{ocscp_nf_instance_id="6faf1bbc-6e4a-4454-a507-a14ef8e1bc5c"} ocscp_metric_upstream_service_time{ocscp_service_instance_id="fe137ab7-740a-46ee-aa5c-951806d77b02"} ocscp_metric_upstream_service_time{ocscp_upstream_service_time="1ms"}

Table 5-4 (Cont.) Metrics Reference

Prometheus Stat Metric Name	Metric Description	Dimensions	Example usage to filter metric by dimension on Grafana GUI
ocscp_metric_request_header_to_body_time	This metric captures the time between receiving the request headers to receiving the request body in time buckets (e.g., 1ms, 2ms, 4ms, 8ms and so on)	ocscp_nf_type (e.g., UDM, PCF, AMF, etc.) ocscp_nf_service_type (e.g., nudm-uecm, nudm-sdm, etc.) ocscp_nf_end_point (Default value = 0.0:00) ocscp_locality (SCP site name e.g., Loc6, Loc7, etc.) ocscp_nf_instance_id (e.g., 6faf1bbc-6e4a-4454-a507-a14ef8e1bc5c, etc. Default value = NA) ocscp_service_instance_id (e.g., fe137ab7-740a-46ee-aa5c-951806d77b02, etc. Default value = NA) ocscp_header_to_body_time (e.g., 1ms, 2ms, 4ms, 8ms, etc.)	ocscp_metric_request_header_to_body_time{ocscp_nf_type="UDM"} ocscp_metric_request_header_to_body_time{ocscp_nf_service_type="nudm-uecm"} ocscp_metric_request_header_to_body_time{ocscp_nf_end_point="10.96.166.65:80"} ocscp_metric_request_header_to_body_time{ocscp_locality="Loc7"} ocscp_metric_request_header_to_body_time{ocscp_nf_instance_id="6faf1bbc-6e4a-4454-a507-a14ef8e1bc5c"} ocscp_metric_request_header_to_body_time{ocscp_service_instance_id="fe137ab7-740a-46ee-aa5c-951806d77b02"} ocscp_metric_request_header_to_body_time{ocscp_header_to_body_time="1ms"}

Table 5-4 (Cont.) Metrics Reference

Prometheus Stat Metric Name	Metric Description	Dimensions	Example usage to filter metric by dimension on Grafana GUI
ocscp_metric_request_complete_time	This metric captures the time of receiving the complete request in time buckets (e.g., 1ms, 2ms, 4ms, 8ms and so on)	ocscp_nf_type (e.g., UDM, PCF, AMF, etc.) ocscp_nf_service_type (e.g., nudm-uecm, nudm-sdm, etc.) ocscp_nf_end_point (Default value = 0.0:00) ocscp_locality (SCP site name e.g., Loc6, Loc7, etc.) ocscp_nf_instance_id (e.g., 6faf1bbc-6e4a-4454-a507-a14ef8e1bc5c, etc. Default value = NA) ocscp_service_instance_id (e.g., fe137ab7-740a-46ee-aa5c-951806d77b02, etc. Default value = NA) ocscp_request_complete_time (e.g., 1ms, 2ms, 4ms, 8ms, etc.)	ocscp_metric_request_complete_time{ocscp_nf_type="UDM"} ocscp_metric_request_complete_time{ocscp_nf_service_type="nudm-uecm"} ocscp_metric_request_complete_time{ocscp_nf_end_point="10.96.166.65:80"} ocscp_metric_request_complete_time{ocscp_locality="Loc7"} ocscp_metric_request_complete_time{ocscp_nf_instance_id="6faf1bbc-6e4a-4454-a507-a14ef8e1bc5c"} ocscp_metric_request_complete_time{ocscp_service_instance_id="fe137ab7-740a-46ee-aa5c-951806d77b02"} ocscp_metric_request_complete_time{ocscp_request_complete_time="1ms"}
ocscp_metric_downstream_connection	Total number of downstream connections per thread.	ocscp_thread_id (Thread Id of the thread which is handling the connection)	ocscp_metric_downstream_connection{ocscp_thread_id ="23434434234"}
ocscp_metric_total_http_rx_downstream_req	Total number of incoming HTTP requests per downstream peers	ocscp_nf_type (e.g., UDM, PCF, AMF, etc.) ocscp_nf_service_type (e.g., nudm-uecm, nudm-sdm, etc.) ocscp_thread_id (Thread Id of the thread which is processing the request) ocscp_locality (SCP site name e.g., Loc6, Loc7, etc.) ocscp_downstream_remote_address (IP address ("-" separated instead of ".") of downstream peer e.g. 10-233-73-63)	ocscp_metric_total_http_rx_downstream_req{ocscp_nf_type="UDM"} ocscp_metric_total_http_rx_downstream_req{ocscp_nf_service_type="nudm-uecm"} ocscp_metric_total_http_rx_downstream_req{ocscp_thread_id ="23434434234"} ocscp_metric_total_http_rx_downstream_req{ocscp_locality="Loc7"} ocscp_metric_total_http_rx_downstream_req{ocscp_downstream_remote_address ="10-233-73-63"}

Table 5-4 (Cont.) Metrics Reference

Prometheus Stat Metric Name	Metric Description	Dimensions	Example usage to filter metric by dimension on Grafana GUI
ocscp_upstream_app_service_time_ms	Bucketed response time by SCP APPS as per allowed dimensions. For mediation, ocscp_app_name is 'nmediation-http' for ocscp_upstream_service_time, buckets(ms) are = 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024, 2048	ocscp_app_name (nmediation_http, ocscp-sds-amf and ocscp-sds-smf) ocscp_upstream_service_time (e.g., 1ms, 2ms, 4ms, 8ms, etc.)	ocscp_nf_type ocscp_nf_service_type ocscp_app_name ocscp_trigger_name ocscp_upstream_service_time
ocscp_metric_total_mediation_processing_failures	Number of processing failures at nf-mediation service.	NA	NA
ocscp_metric_downstream_request_reset	For downstream message got reset at scp, this metrics calculate bucketed elapsed time of such message at SCP. Time Buckets are 1ms,2ms,4ms, 8ms, to 2048ms.	ocscp_elapsed_time(Example: 1ms, 2ms, 4ms, 8ms, etc.)	sum(ocscp_metric_downstream_request_reset) by (ocscp_elapsed_time)
ocscp_metric_scp_generated_response	Captures the error response generated by SCP.	• ocscp_nf_type(Example: UDM, PCF, AMF, etc.) • ocscp_nf_service_type(Example: nudm-uecm, nudm-sdm, etc.) • ocscp_response_code(Example: 503, 404,408, etc.) • ocscp_error_group(Example: ocscp.http.config_error.cluster_not_found, ocscp.http.routing_failure.connect_failure, etc)	ocscp_metric_scp_generated_response{ocscp_nf_type="UDM",ocscp_nf_service_type="nudm-uecm",ocscp_response_code="503",ocscp_error_group="ocscp.http.routing_failure.connect_failure"}

Table 5-4 (Cont.) Metrics Reference

Prometheus Stat Metric Name	Metric Description	Dimensions	Example usage to filter metric by dimension on Grafana GUI
ocscp_metric_config_error_cluster_not_found	Captures cluster name (destination endpoint), which is not get configured properly at SCP.	ocscp_cluster_name (Example: outbound|80|| udm1svctest_default_svc_cluster_local)	ocscp_metric_config_error_cluster_not_found{ocscp_cluster_name="outbound|80|| udm1svctest_default_svc_cluster_local"} **Note:** This metric is relevant for internal debugging purpose, as it has to show cluster name which is used by SCP, but might not similar to what user has configured in nf_profile.

Traces Reference

The following table provides information for Traces for Service Communication Proxy.

Table 5-5 Traces Reference

Field Name	Request/ Response Type	Description
component	common	The software package, framework, library, or module that generated the associated Span.
node_id	common	Local information
method	request,common	HTTP method of the request for the associated Span. Example: "GET","POST"
scheme	request	Url scheme is http
authority	request	Authority give you details about registered name or server address, along with optional port and user information
path	request	A path consists of a sequence of path segments separated by a slash ("/") character.
3gpp-sbi-message-priority	request	This header shall be included in HTTP/2 messages when a priority for the message needs to be conveyed
x-forwarded-for	request	To identify the originating IP address of a client.
x-forwarded-proto	request	To determine the protocol used between the client and the spf.

Table 5-5 (Cont.) Traces Reference

Field Name	Request/ Response Type	Description
x-envoy-internal	request	service wants to know whether a request is internal origin or not
via	request	It is used for tracking message forwards, avoiding request loops, and identifying the protocol capabilities of senders along the request/ response chain
x-request-id	common	The x-request-idheader is used to uniquely identify a request as well as perform stable access logging and tracing
payload	request, common	http request body.
status	response	To determine the http request has been succeeded or not.
content-type	response	The Content-Type entity header is used to indicate the media type of the resource
content-length	response	The Content-Length header indicates the size of the entity body in the message, in bytes
server	response	The Server response-header field contains information about the software used by the origin server to handle the request
date	response	The time and date, when the request is processed.
x-envoy-upstream-service-time	response	Contains the time in milliseconds spent by the upstream host processing the request
location	response	To provide information about the location of a newly created resource
payload	response	http response body.
http.url	request,common	Specifies the request's URL.
downstream_cluster	common	A downstream host connects to Envoy, sends requests, and receives responses
user_agent	request,common	When your browser connects to a website, it includes a User-Agentfield in itsHTTPheader
http.protocol	common	The communication between client and server over HTTP/2.
request_size	common	HTTP header size.

Table 5-5 (Cont.) Traces Reference

Field Name	Request/ Response Type	Description
upstream_cluster	common	An upstream host receives connections and requests from Envoy and returns responses.
http.ststus_code	common	HTTP response status code for the associated Span. Example: 200, 503, 404
response_size	common	HTTP header size.
response_flag	common	Additional details about the response or connection, if any
span.kind	common	Specifies the role of the Span in a RPC communication. In the case of HTTP communication it is seeingclientandservervalues for this tag.
error	common	True, if and only if, the application considers the operation represented by the Span to have failed
x-request-id	request	The x-request-idheader is used by Envoy to uniquely identify a request as well as perform stable access logging and tracing
x-b3-traceid	request	The x-b3-traceidHTTP header is used by the Zipkin tracer in Envoy. The TraceId is 64-bit in length and indicates the overall ID of the trace. Every span in a trace shares this ID
x-b3-spanid	request	The x-b3-spanidHTTP header is used by the Zipkin tracer in Envoy. The SpanId is 64-bit in length and indicates the position of the current operation in the trace tree
x-b3-sampled	request	The x-b3-sampledHTTP header is used by the Zipkin tracer in Envoy. When the Sampled flag is either not specified or set to 1, the span will be reported to the tracing system
ueidentitytype	request	NF type.
ueidentityvalue	request	supi range for NF type .
x-envoy-expected-rq-timeout-ms	request	This is the time in milliseconds the router expects the request to be completed

HTTP Status Code and applicability for rerouting

Description

This page describes the HTTP status codes usage on SBI. HTTP status codes are carried in ":status" pseudo header field in HTTP/2, as defined in subclause 8.1.2.4 in IETF RFC 7540.

Below table specifies HTTP status codes per HTTP method which is supported on SBI. Support of an HTTP status code is:

- Mandatory, which is marked in table as "**M**". This means that all 3GPP NFs shall support the processing of the specific HTTP status code for the specific HTTP method, when received in a HTTP response message. In such cases the 3GPP NF also supports the handling of the "ProblemDetails" JSON object with the Content-Type header field set to the value "application/problem+json" for HTTP status codes 4xx and 5xx, if the corresponding API definition in the related technical specification does not specify another response body for the corresponding status code;
- Service specific, which is marked in table as "**SS**" and means that the requirement to process the HTTP status code depends on the definition of the specific API; or
- Not applicable, which is marked in table as "**N/A**". This means that the specific HTTP status code shall not be used for the specific HTTP method within the 3GPP NFs.
- Applicable for Rerouting column describes if the status code is applicable for rerouting at SPF. These Status codes can be configured in Routing options for each NF services.

NOTE 1: "200 OK" response used on SBI shall contain body.

NOTE 2: If the NF acting as an HTTP Client receives 2xx response code not appearing in table, the NF shall treat the received 2xx response: - as "204 No Content" if 2xx response does not contain body; and - as "200 OK" if 2xx response contains body.

HTTP status code supported on SBI

Table 5-6 HTTP status code supported on SBI

HTTP status code	HTTP status code					HTTP method	Applicable for Rerouting
	DELETE	GET	PATCH	POST	PUT		
100 Continue	N/A	N/A	N/A	N/A	N/A	No	
200 OK (NOTE 1)	SS	M	SS	SS	SS	No	
201 Created	N/A	N/A	N/A	SS	SS	No	
202 Accepted	SS	N/A	SS	SS	SS	No	
204 No Content (NOTE 2)	M	N/A	SS	SS	SS	No	
300 Multiple Choices	N/A	N/A	N/A	N/A	N/A	No	

Table 5-6 (Cont.) HTTP status code supported on SBI

303 See Other	SS	SS	N/A	SS	SS	NO	
307 Temporary Redirect	SS	SS	SS	SS	SS	Yes	307 (Should be included as part of 3xx)
308 Permanent Redirect	SS	SS	SS	SS	SS	Yes	308 (Should be included as part of 3xx)
400 Bad Request	M	M	M	M	M	No	
401 Unauthorized	M	M	M	M	M	No	
403 Forbidden	SS	SS	SS	SS	SS	No	
404 Not Found	SS	SS	SS	SS	SS	Yes	404
405 Method Not Allowed	SS	SS	SS	SS	SS	No	
406 Not Acceptable	N/A	N/A	N/A	N/A	N/A	No	
408 Request Timeout	SS	SS	SS	SS	SS	Yes	408
409 Conflict	N/A	N/A	SS	SS	SS	Yes	409 (should be included as part of "retriable-4xx")
410 Gone	SS	SS	SS	SS	SS	Yes	410
411 Length Required	N/A	N/A	M	M	M	No	
412 Precondition Failed	SS	SS	SS	SS	SS	No	
413 Payload Too Large	N/A	N/A	M	M	M	No	
414 URI Too Long	N/A	M	N/A	N/A	N/A	No	
415 Unsupported Media Type	N/A	N/A	M	M	M	No	
500 Internal Server Error	M	M	M	M	M	Yes	500
501 Not Implemented	SS	SS	SS	SS	SS	Yes	501
503 Service Unavailable	M	M	M	M	M	Yes	503 (Should be included as part of "5xx")
504 Gateway Timeout	SS	SS	SS	SS	SS	Yes	504 (Should be included as part of "5xx")

NF as HTTP Client

Besides the HTTP Status Codes defined in the API specification, a NF as HTTP client should support handling of 1xx, 3xx, 4xx and 5xx HTTP Status Codes specified in above table, following the client behavior in corresponding IETF RFC where the received HTTP Status Code is defined.

When receiving a not recommended or not recognized 1xx, 3xx, 4xx or 5xx HTTP Status Code, a NF as HTTP client should treat it as x00 status code of the class, as described in clause 6 of IETF RFC 7231.

If 100, 200/204, 300, 400 or 500 response code is not defined by the API specification, the client may follow guidelines below:

- For 1xx (Informational):
  - Discard the response and wait for final response.
- For 2xx (Successful):
  - Consider the service operation is successful if no mandatory information is expected from the response payload in subsequent procedure.
  - If mandatory information is expected from response payload in subsequent procedure, parse the payload following description in subclause 6.2.1 of IETF RFC 7231 [11]. If parse is successful and mandatory information is extracted, continue with subsequent procedure.
  - Otherwise, consider service operation has failure and start failure handling.
- For 3xx (Redirection):
  - Retry the request towards the directed resource referred in the Location header, using same request method.
- For 4xx (Client Error):
  - Validate the request message and make correction before resending. Otherwise, stop process and go to error handling procedure.
- For 5xx (Server Error):
  - Stop process and go to error handling process.

NF as HTTP Server

A NF acting as an HTTP server is able to generate HTTP status codes specified in above table per indicated HTTP method.

An HTTP method which is not supported by 5GC SBI API specification is rejected with the HTTP status code "501 Not Implemented".

NOTE 1: In this case, the NF does not need to include in the HTTP response the "cause" attribute indicating corresponding error since the HTTP status code "501 Not Implemented" itself provides enough information of the error, i.e. the NF does not recognize the HTTP method.

If the specified target resource does not exist, the NF rejects the HTTP method with the HTTP status code "404 Not Found".

If the NF supports the HTTP method but not by a target resource, the NF rejects the HTTP method with the HTTP status code "405 Method Not Allowed" and includes in the response an Allow header field containing the supported method(s) for that resource.

NOTE 2: In this case, the NF does not need to include in the HTTP response the "cause" attribute indicating corresponding error since the HTTP status code "405 Method Not Allowed" itself provides enough information of the error and hence the Allow header field lists HTTP method(s) supported by the target resource.

If the received HTTP request contains incorrect optional IE, the NF discards the incorrect IE.

If the NF supports the HTTP method by a target resource but the NF cannot successfully fulfil the received request, the following requirements apply.

A NF as HTTP Server should map application errors to the most similar 3xx/4xx/5xx HTTP status code specified in table 5.2.7.1-1. If no such code is applicable, it should use "400 Bad Request" status code for errors caused by client side or "500 Server Internal Error" status code for errors caused on server side.

If the received HTTP request contains unsupported payload format, the NF rejects the HTTP request with the HTTP status code "415 Unsupported Media Type". If the HTTP PATCH method is rejected, the NF includes the Accept-Patch header field set to the value of supported patch document media types for a target resource i.e. to "application/merge-patch+json" if the NF supports "JSON Merge Patch" and to "application/json-patch+json" if the NF supports "JSON Patch". If the received HTTP PATCH request contains both "JSON Merge Patch" and "JSON Patch" documents and the NF supports only one of them, the NF ignores unsupported patch document.

NOTE 3: The format problem might be due to the request's indicated Content-Type or Content-Encoding header fields, or as a result of inspecting the payload body directly.

If the received HTTP request contains payload body larger than the NF is able to process, the NF rejects the HTTP request with the HTTP status code "413 Payload Too Large".

If the result of the received HTTP POST request used for a resource creation would be equivalent to the existing resource, the NF rejects the HTTP request with the HTTP status code "303 See Other" and includes in the HTTP response a Location header field set to the URI of the existing resource.

Protocol and application errors common to several 5GC SBI API specifications for which the NF includes in the HTTP response a payload body ("ProblemDetails" data structure or application specific error data structure) with the "cause" attribute indicating corresponding error are listed in below table.

Table 5-7 Protocol and application errors

Parameters	HTTP status code	Description
INVALID_API	400 Bad Request	The HTTP request contains an unsupported API name or API version in the URI.
INVALID_MSG_FORMAT	400 Bad Request	The HTTP request has an invalid format.
INVALID_QUERY_PARAM	400 Bad Request	The HTTP request contains an unsupported query parameter in the URI.
MANDATORY_IE_INCORRECT	400 Bad Request	A mandatory IE or conditional IE in data structure, but mandatory required, for an HTTP method was received with a semantically incorrect value. (NOTE 1)

Table 5-7 (Cont.) Protocol and application errors

Parameters	HTTP status code	Description
MANDATORY_IE_MISSING	400 Bad Request	IE which is defined as mandatory or as conditional in data structure, but mandatory required, for an HTTP method is not included in the payload body of the request. (NOTE 1)
UNSPECIFIED_MSG_FAILURE	400 Bad Request	The request is rejected due to unspecified client error. (NOTE 2)
MODIFICATION_NOT_ALLOWED	403 Forbidden	The request is rejected because the contained modification instructions attempt to modify IE which is not allowed to be modified.
SUBSCRIPTION_NOT_FOUND	404 Not Found	The request for modification or deletion of subscription is rejected because the subscription is not found in the NF.
RESOURCE_URI_STRUCTURE_NOT_FOUND	404 Not Found	The request is rejected because a fixed part after the first variable part of an "apiSpecificResourceUriPart" (as defined in subclause 4.4.1 of 3GPP TS 29.501) is not found in the NF. This fixed part of the URI may represent a sub-resource collection (e.g. contexts, subscriptions, policies) or a custom operation. (NOTE X)
INCORRECT_LENGTH	411 Length Required	The request is rejected due to incorrect value of a Content-length header field.
NF_CONGESTION_RISK	429 Too Many Requests	The request is rejected due to excessive traffic which, if continued over time, may lead to (or may increase) an overload situation.
INSUFFICIENT_RESOURCES	500 Internal Server Error	The request is rejected due to insufficient resources.
UNSPECIFIED_NF_FAILURE	500 Internal Server Error	The request is rejected due to unspecified reason at the NF. (NOTE 3)
SYSTEM_FAILURE	500 Internal Server Error	The request is rejected due to generic error condition in the NF.
NF_CONGESTION	503 Service Unavailable	The NF experiences congestion and performs overload control, which does not allow the request to be processed. (NOTE 4)

NOTE 1: "invalidParams" attribute is included in the "ProblemDetails" data structure indicating missing or incorrect IE.

NOTE 2: This application error indicates error in the HTTP request and there is no other application error value that can be used instead.

NOTE 3: This application error indicates error condition in the NF and there is no other application error value that can be used instead.

NOTE 4: If the reason for rejection is a temporary overload, the NF may include in the response a Retry-After header field to indicate how long the service is expected to be unavailable.

NOTE X: If the request is rejected because of an error in an URI before the first variable part of an "apiSpecificResourceUriPart", the "404 Not Found" HTTP status code may be sent without "ProblemDetails" data structure indicating protocol or application error.