Oracle® Communications

Service Communication Proxy (SCP)

Cloud Native User's Guide

Release 1.2.0
F21621-01
September 2019

Oracle Communications Service Communication Proxy (SCP) Cloud Native User's Guide, Release 1.2.0

F21621-01

Contents

List of Figures

List of Tables

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 elements advertise and provide services that can be consumed using REST APIs by other elements in the core. This allows for the adoption of web-scale technologies and software that are used by different organizations in telecom networks.

The SCP Offloads the 5G NFs from below common functionalities load balancing, routing and selection at 5G NFs.

- **Routing/Selection** – Consumers need to define routing rules, refresh cache, and handle application failures/redirects
- **Load Balancing** Based on static capacity, no feedback loop, and NF specific
- **NF Subscription**- Subscription for all producers (change in load, capacity, priority), which may decrease network traffic.
- **NF Degradation and Failures** – Timeouts can result in cascaded failures, need for circuit breaker
- **Traffic Prioritization** - Message Priority assignment
- **Congestion and Overload** - Provides uniform load balancing/routing strategy across the network. Protects the pod (server) from overload with respect to various system resources.
- Dynamic discovery of 5G Topology from NRF and creation of routing rules.

The Oracle Communications Service Communication Proxy brings telecom awareness to the service mesh and helps resolve the above issues in the 5G core network.

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
EFK stack	Elasticsearch, Fluentd, and Kibana stack

Table 1-1 (Cont.) Acronyms and Terminologies

Field	Description
FQDN	Fully Qualified Domain Name
GPSI	Generic Public Subscription Identifier
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
SEPP	Security Edge Protection Proxy
SMF	Session Management Function
SUPI	Subscription Permanent Identifier
UDR	Unified Data Repository
UDSF	Unstructured Data Storage Function

Terminology

The following table provides the terms and their definitions used in this document.

Table 1-2 Terminology

Term	Description
Downstream Host	A downstream host connects to SCP, sends requests, and receives responses
Upstream Host	An upstream host receives connections and requests from SCP and returns responses.

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.

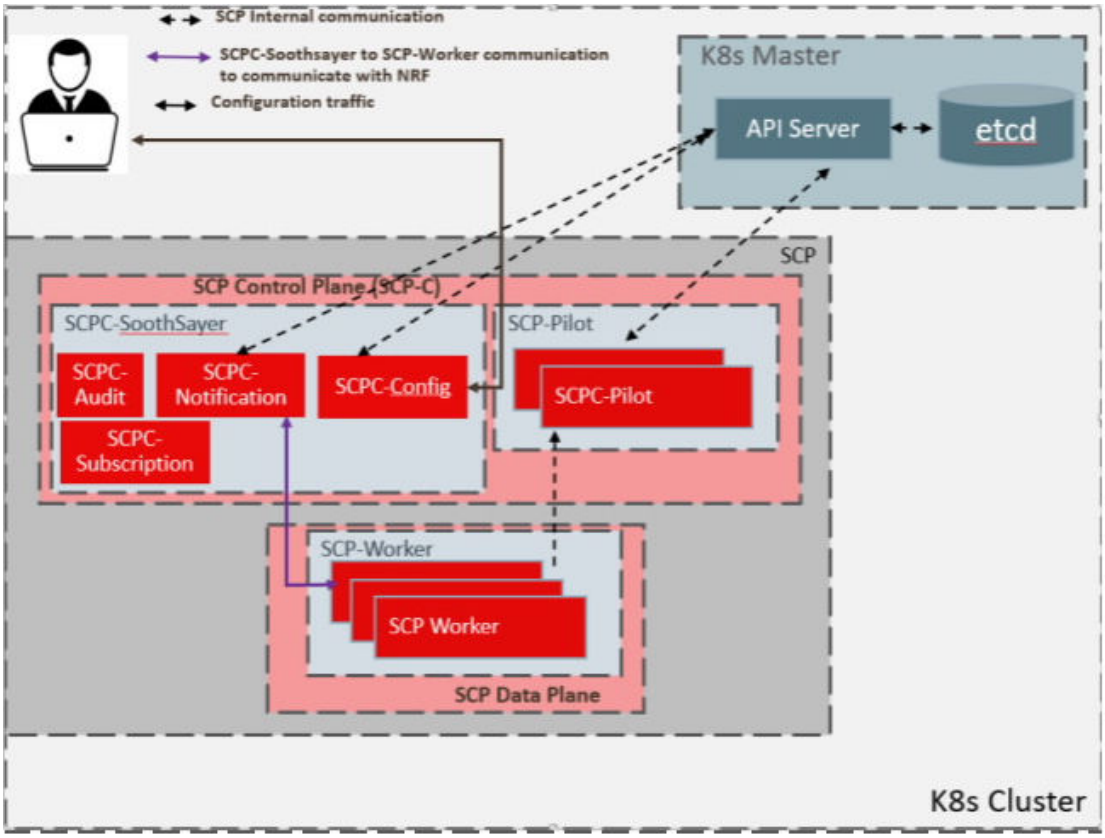
2

Service Communication Proxy System 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. The Service Communication Proxy has a control plane and a data plane.

Figure 2-1 Service Communication Proxy Architecture



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
- Routing Control

- Message Priority Assignment/Override
- Circuit Breaking and Outlier Detection
- Overload Control
- Observability

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 an 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 schemes such as round robin, weighted round robin, transaction latency, etc while factoring in the current load and NF availability.

Routing Control

By leveraging its position in the network, the 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.

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 can also perform 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.

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 and controller supports overload control based on the usage of below listed resources:

- Memory
- CPU
- File descriptors

The SCP worker and controller considers itself to be overloaded if the usage associated with memory, CPU or File descriptors 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).

> **Note:**
>
> Currently, only Memory overload control is handled.

Observability

The following are available in observability.

- **Metrics**
  Metrics services requests are proxied through the Service Communication Proxy, the Service Proxy Controller can collect 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 Metrics, KPIs, and Traces.
- **Tracing**
  Compliant with open API tracing
- **Logging**
  Compliant with EFK stack.

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 configuration interfaces:

- **Signaling Interface**
  - Signaling interface is exposed by SCP data plane (i.e. SCP Worker) and this interface will be used to receive all 5G signaling traffic.
- **Config Interface**
  - Config interface is exposed by SCP control plane (i.e. 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 of 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 need 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" = 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.
- **Port**
  - Consumer NFs need port info 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 info along with fqdn/ip address to configure the SCP for routing.
  - Port is 8081 i.e. fixed port (not configurable).

Configuring CanaryRelease Options

Canary testing involves simultaneous deployment of both old release and new release software into a production network and then splitting the production workload such a way that just a small fraction goes to the new release while the majority of the workload continues to be directed at the old release. The KPIs of the new release software is monitored, and if passes the criteria, then the canary release is removed and the *main* (old) release is upgraded. If the new release software fails, then it is removed, and developers are alerted.

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. The older version is considered the production version and the newer version of the service instance is considered the *canary* release and the SCP distributes traffic between Production version and the Canary versions based on operator configuration

User can configure CanaryRelease options by following the information provided in the table below. The supported operations are **LIST**, **GET**, and **PATCH**.
Table 3-1 provides details about the operations and parameters for CanarayRelease Options. The default values of parameters related to CanaryRelease are mentioned in the following table, however, User can modify the values. These parameters are applicable at POD level.

Table 3-1 Configuring Parameters for CanaryRelease Options

Method	Scheme	Field Name	Type	Authority	Port	Path	Parameters/Command	Description

GET	http	-	-	<SCP config service fqdn>	8081	/soothsayer/v1/canaryrelease/	[{
							"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
							
							}
							
							...
							
							]
								-

Table 3-1 (Cont.) Configuring Parameters for CanaryRelease Options

Method	Scheme	Field Name	Type	Authority	Port	Path	Parameters/Command	Description

LIST	-	-	-	-	-	-	`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 } ... ]`
								-

PATCH	-	canaryReleaseFlag	Boolean	-	-	-	Set the value of field canaryReleaseFlag and mention serviceName for which the configuration is needed in the resource path of below Curl Command. **canaryReleaseFlag UPDATE Command** `curl --header "Content-Type: application/json" --request PATCH --data '{ "canaryReleaseFlag": true }' http://<SCP config service fqdn>:8081/soothsayer/v1/canaryrelease/<serviceName>`	Enable/ Disable canary release support. **Default Value**: null

Table 3-1 (Cont.) Configuring Parameters for CanaryRelease Options

Method	Scheme	Field Name	Type	Authority	Port	Path	Parameters/Command	Description
		apiFullVersion	String	-	-	-	Set the value of field apiFullVersion and mention serviceName for which the configuration is needed in the resource path of below Curl Command. **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>`	The API full version of the canary service. **Default Value**: null
		canaryTraffic	Integer	-	-	-	Set the value of field canaryTraffic and mention serviceName for which the configuration is needed in the resource path of below Curl Command. **canaryTraffic UPDATE Command** `curl --header "Content-Type: application/json" --request PATCH --data '{ "canaryTraffic": 10 }' http://<SCP config service fqdn>:8081/soothsayer/v1/canaryrelease/<serviceName>`	The traffic that should be distributed to Canary release. **Default Value**: null

Configuring Routing Options

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

Parameters for Configuring Routing Options

Table 3-2 provides details of the parameters for configuring Routing Options.

Table 3-2 Parameters for RoutingOptions

Parameter Name	Description	Applicable to NF Service Type	Default Values	Applicable to Pod level within NF	Values
Max Pending responses	Number of pending responses from NF/Pod	Yes	1000	Yes	1000
Response Timeout	When response timeout expires, then SCP initiates alternate rerouting to available alternate NF or Pod.	Yes	1 second	Yes	1 second
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	Yes	6 seconds
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	Yes	2

Table 3-2 (Cont.) Parameters for RoutingOptions

Parameter Name	Description	Applicable to NF Service Type	Default Values	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) – Complete list of supported HTTP status code is at HTTP Status Code and applicability for rerouting. • 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)	-	• 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		
Alternate Routing	Alternate rerouting is Enabled or Disabled • Reroute to alternate Pod (within same NF) • Reroute to alternate producer NF	Yes	Enabled	Yes	Enabled
Request Routing Scope	Site	Yes	Site	Yes	Within NF
Status	• No Sync • Site Wide • Mated Pair • N/W Wide	Yes	No Sync	Yes	Synced within NF

Table 3-2 (Cont.) Parameters for RoutingOptions

Parameter Name	Description	Applicable to NF Service Type	Default Values	Applicable to Pod level within NF	Values
Routing Policy	• Forward Request – Forward Request(Use consumer's orig. destination unless available) • Load Balance (Consumer selected site first) • Load Balance (LB Across sites)	Yes	Forward Proxy	NO	Load Balance (Non-configurable)
Deployment Info (deploymentInfo)	• deploymentInfo • chfDeploymentInfo • chfDeploymentModel	Yes		No	
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	-
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	-

Table 3-2 (Cont.) Parameters for RoutingOptions

Parameter Name	Description	Applicable to NF Service Type	Default Values	Applicable to Pod level within NF	Values
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. For setting reverseProxySupport as true dbSync status should be "Site_Wide" and routingPolicy should be "Load_Balance". dbSync status should be synced and it can take other values except No_Sync.	Yes	false	No	true, false
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	
	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	

Table 3-2 (Cont.) Parameters for RoutingOptions

Parameter Name	Description	Applicable to NF Service Type	Default Values	Applicable to Pod level within NF	Values
	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	

Deployment Info

Currently only CHF is supporting this deploymentInfo. DeploymentInfo is of type **chfDeploymentInfo**.

Table 3-3 deploymentInfo

Attribute Name	Data Type	P	Cardinality	Description
chfDeploymentInfo	chfDeploymentInfo	O	1	CHF deployment scenario, populated only in case on CHF NF services.

This attribute is applicable for CHF NF services and it defines the CHF deployment model i.e. operator has deployed the CHF instances in the network.

Table 3-4 chfDeploymentInfo

Attribute Name	Data Type	P	Cardinality	Description
chfDeploymentModel	chfDeploymentModel	M	1	CHF deployment scenario, populated only in case on CHF NF services.
subsequentRequestReroutingEnabled	boolean	O	1	This attribute indicates whether rerouting of subsequent CHF service requests are enabled or not. • true, (Operator may chose to enable, if Primary and Secondary CHF instances share data) • false, (Operator may chose to disable, if Primary and Secondary CHF instances do not share data)

Table 3-5 chfDeploymentModel

Enumeration value	CHF Deployment
REGIONAL	Regional CHF deployment i.e. CHFs are deployed in Primary region and Secondary region. A region may consist of one or more locality.
SITE_WIDE	Site specific CHF deployment i.e. CHF instances are deployed as per SCP's Site deployment.

Configuring Operations for Routing Options

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

Table 3-6 provides sample details of the operations to configure routing options.

Table 3-6 Routing Options Operations

Operation	REST Command

LIST	curl --header 'Content-type: application/json' --header 'accept: application/json' --request GET http://<Soothsayerfqdn>:8081/soothsayer/v1/routingoptions/
	
	[{
	"pod": {
	"maxPendingResponses": 1000,
	"maxRoutingAttempts": 2,
	"alternateRouting": true,
	"loadBalancingAlgorithm": "Round_Robin"
	},
	"srv": {
	"name": "nudm-uecm",
	"maxPendingResponses": 1000,
	"maxRoutingAttempts": 3,
	"actions": "Forward",
	"alternateRouting": true,
	"scope": "Site",
	"dbSyncStatus": "No_Sync",
	"routingPolicy": "Forward_Proxy",
	"loadBalancingAlgorithm": "Priority_only",
	
	"nfServiceLoadBasedCongestionControl": {
	
	"alternateRoutingOnsetThresholdPercent": 80,
	
	"alternateRoutingAbatementThresholdPercent": 75,

Table 3-6 (Cont.) Routing Options Operations

Operation	REST Command
	"throttleOnsetThresholdPercent": 90, "throttleOnsetThresholdPercent": 85, "responseErrorCode": 503 }, "defaultPriority": 1, "defaultCapacity": 65535, "reverseProxySupport": false }, "totalTransactionLifetime": "6s", "reRouteOnResponseCodeList": ["ALL_SERVER_ERROR", "NOT_FOUND", "REQUEST_TIMEOUT", "RETRIABLE_4XX", "GONE", "TOO_MANY_REQUESTS", "TEMPORARY_REDIRECT", "PERMANENT_REDIRECT"], "responseTimeout": "1s" }, ...]

Table 3-6 (Cont.) Routing Options Operations

Operation	REST Command

GET	curl --header 'Content-type: application/json' --header 'accept: application/json' --request GET http://<Soothsayerfqdn>:8081/soothsayer/v1/routingoptions/<serviceName>
	
	{
	
	"pod": {
	
	"maxPendingResponses": 1000,
	
	"maxRoutingAttempts": 2,
	
	"alternateRouting": true,
	
	"loadBalancingAlgorithm": "Round_Robin"
	
	},
	
	"srv": {
	
	"name": "nudm-uecm",
	
	"maxPendingResponses": 1000,
	
	"maxRoutingAttempts": 3,
	
	"actions": "Forward",
	
	"alternateRouting": true,
	
	"scope": "Site",
	
	"dbSyncStatus": "No_Sync",
	
	"routingPolicy": "Forward_Proxy",
	
	"loadBalancingAlgorithm": "Priority_only",
	
	"nfServiceLoadBasedCongestionControl": {
	
	"alternateRoutingOnsetThresholdPercent": 80,
	
	"alternateRoutingAbatementThresholdPercent": 75,

Table 3-6 (Cont.) Routing Options Operations

Operation	REST Command
	"throttleOnsetThresholdPercent": 90, "throttleAbatementThresholdPercent": 85, "responseErrorCode": 503 }, "defaultPriority": 1, "defaultCapacity": 65535, "reverseProxySupport": false }, "totalTransactionLifetime": "6s", "reRouteOnResponseCodeList": ["ALL_SERVER_ERROR", "NOT_FOUND", "REQUEST_TIMEOUT", "RETRIABLE_4XX", "GONE", "TOO_MANY_REQUESTS", "TEMPORARY_REDIRECT", "PERMANENT_REDIRECT"], "responseTimeout": "1s" }

Table 3-6 (Cont.) Routing Options Operations

Operation	REST Command

PUT	curl --header "Content-Type: application/json" --request PUT --data '{
	"pod": {
	"maxPendingResponses": 1000,
	"maxRoutingAttempts": 2,
	"alternateRouting": true,
	"loadBalancingAlgorithm": "Round_Robin"
	},
	"srv": {
	"name": "nudm-uecm",
	"maxPendingResponses": 1000,
	"maxRoutingAttempts": 3,
	"actions": "Forward",
	"alternateRouting": true,
	"scope": "Site",
	"dbSyncStatus": "No_Sync",
	"routingPolicy": "Forward_Proxy",
	"loadBalancingAlgorithm": "Priority_only",
	"nfServiceLoadBasedCongestionControl": {
	"alternateRoutingOnsetThresholdPercent": 80,
	"alternateRoutingAbatementThresholdPercent": 75,
	"throttleOnsetThresholdPercent": 90,

Table 3-6 (Cont.) Routing Options Operations

Operation	REST Command
	"throttleAbatementThresholdPercent": 85, "responseErrorCode": 503 }, "defaultPriority": 1, "defaultCapacity": 65535, "reverseProxySupport": false }, "totalTransactionLifetime": "6s", "reRouteOnResponseCodeList": ["ALL_SERVER_ERROR", "NOT_FOUND", "REQUEST_TIMEOUT", "RETRIABLE_4XX", "GONE", "TOO_MANY_REQUESTS", "TEMPORARY_REDIRECT", "PERMANENT_REDIRECT"], "responseTimeout": "1s" }' http://<Soothsayerfqdn>:8081/soothsayer/v1/routingoptions/<serviceName>

Table 3-6 (Cont.) Routing Options Operations

Operation	REST Command

PATCH	curl -X PATCH \
	http://<Soothsayerfqdn>:8081/soothsayer/v1/routingoptions/<service name> \
	-H 'Content-Type: application/merge-patch+json' \
	-d
	
	{
	"pod":{
	"maxPendingResponses":500,
	"maxRoutingAttempts":2,
	"alternateRouting":true,
	
	"loadBalancingAlgorithm":"Round_Robin"
	},
	"srv":{
	"name":"nchf-spendinglimitcontrol",
	"maxPendingResponses":1000,
	"maxRoutingAttempts":3,
	"actions":"Forward",
	"alternateRouting":true,
	"scope":"Site",
	"dbSyncStatus":"No_Sync",
	"routingPolicy":"Forward_Proxy",
	
	"loadBalancingAlgorithm":"Priority_only",
	
	"nfServiceLoadBasedCongestionControl":{
	
	"alternateRoutingOnsetThresholdPercent":80,
	
	"alternateRoutingAbatementThresholdPercent":75,
	
	"throttleOnsetThresholdPercent":65,
	
	"throttleAbatementThresholdPercent":92,
	"responseErrorCode":404
	},
	"defaultPriority":1,
	"defaultCapacity":65535,
	"reverseProxySupport":false,
	"chfDeploymentInfo":{
	
	"chfDeploymentModel":"regional",
	
	"subsequentRequestReroutingEnabled":false
	}
	},

Table 3-6 (Cont.) Routing Options Operations

Operation	REST Command

	<pre>"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"
	}
	]
	}</pre>

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

- 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's not an E2E mechanism so to have it:

- 3gpp-Sbi-Message-Priority header contains the HTTP/2 message priority value anything between1 to 256. The default is16.

Table 3-7 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 3-7 (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,
				"headerValue": ""
				}
				}
				]

Table 3-7 (Cont.) Configuring Parameters for MessagePriority Options

Operation	Parameter	Type	Description	REST Command
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** `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 3-7 (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 3-7 (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 3-7 (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 3-7 (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 3-7 (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 3-7 (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 3-7 (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 Http2 Protocol Options

SCP allows the user to set HTTP2 options parameter system-wide. The user can configure Http2 protocol options by using the operations **GET**, and **PUT**.

Table 3-8 provides Http2 Protocol Options for scp-gateway.

Table 3-8 Configuring Http2 Protocol Options

Operation	Parameter	Type	Description with Default Values	REST Command

GET	-	-	-	curl --header 'Content-type: application/json' --header 'accept: application/json' --request GET http://<Soothsayerfqdn>:8081/soothsayer/v1/gatewaydetails/scp-gateway
				
				{
				"servers": [
				{
				"port": {
				"number": 80,
				"name": "http",
				"protocol": "HTTP"
				},
				"hosts": [
				"*"
				],
				
				"ocscpw_http2protocoloptions": {
				
				"ocscpw_max_concurrent_streams": 1000,
				
				"ocscpw_initial_window_size": 65535
				},
				
				"ocscpw_httpprotocoloptions": {
				
				"ocscpw_allow_absolute_url": true
				}
				}
				]
				}

Table 3-8 (Cont.) Configuring Http2 Protocol Options

Operation	Parameter	Type	Description with Default Values	REST Command
PUT	ocspfw_max_concurrent_streams	Integer	Http2 Protocol Options of maximum concurrent streams for spf-gateway **Default Value**: 1000	Set the value of field ocspfw_max_concurrent_streams in the below Curl Command **ocspfw_max_concurrent_streams UPDATE Command** `curl --header "Content-Type: application/json" --request PUT --data '{ "servers": [{ "port": { "number": 80, "name": "http", "protocol": "HTTP" }, "hosts": ["*"], "ocspfw_http2protocoloptions": { "ocspfw_max_concurrent_streams": 1000, "ocspfw_initial_window_size": 65535 } }] }' http://<Soothsayerfqdn>:8081/soothsayer/v1/nrfdetails/soothsayer/v1/gatewaydetails/scp-gateway`

Table 3-8 (Cont.) Configuring Http2 Protocol Options

Operation	Parameter	Type	Description with Default Values	REST Command
	ocspfw_initial_window_size	Integer	Http2 Protocol Options of initial window size for spf-gateway **Default Value**: 65535	Set the value of field ocspfw_initial_window_size in the below Curl Command **ocspfw_initial_window_size** UPDATE Command `curl --header "Content-Type: application/json" --request PUT --data '{ "servers": [{ "port": { "number": 80, "name": "http", "protocol": "HTTP" }, "hosts": ["*"], "ocspfw_http2protocoloptions": { "ocspfw_max_concurrent_streams": 1000, "ocspfw_initial_window_size": 65535 } }] }' http://<Soothsayerfqdn>:8081/soothsayer/v1/nrfdetails/soothsayer/v1/gatewaydetails/scp-gateway`

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.

Table 3-9 provides SystemOptions for PUT operation.

Table 3-9 Configuring Parameters for SystemOptions

Operation	Parameter	Value	Description	Example

GET	-	-	-	curl -X GET http://<Soothsayerfqdn>:8081/soothsayer/v1/systemoptions/{instanceId}
				
				Response:
				{
				"instanceId": "e33ac015-081a-4e25-99c1-d1d6c332246e",
				"cb_and_od_enabled": true,
				"trafficPolicy": {
				"connectionPool": {
				"http": {
				"http2MaxRequests": 1000
				}
				},
				"outlierDetection": {
				"consecutiveErrors": 5,
				"interval": "10s",
				"baseEjectionTime": "30s",
				"maxEjectionPercent": 100
				}
				}
				}

Table 3-9 (Cont.) Configuring Parameters for SystemOptions

Operation	Parameter	Value	Description	Example
PUT	instanceId	String	Unique ID that represents SystemOption record	Set the value of **instanceId** field in the curl command below **instanceId UPDATE Command** `curl -X PUT \ http://<Soothsayerfqdn>:8081/soothsayer/v1/systemoptions \ -H 'Content-Type: application/json' \ -d '{ "instanceId": "e33ac015-081a-4e25-99c1-d1d6c332246e", "cb_and_od_enabled": true, "trafficPolicy": { "connectionPool": { "http": { "http2MaxRequests": 1000 } }, "outlierDetection": { "consecutiveErrors": 5, "interval": "10s", "baseEjectionTime": "30s", "maxEjectionPercent": 100 } } }'`

Table 3-9 (Cont.) Configuring Parameters for SystemOptions

Operation	Parameter	Value	Description	Example

	cb_and_od_enabled	Boolean	Provides information whether the Circuit-Breaking and Outlier-Detection is enabled or not.	Set the value of **cb_and_od_enabled** field in the curl command below
				cd_and_od_enabled UPDATE Command
				`curl -X PUT \`
				` http://<Soothsayerfqdn>:8081/soothsayer/v1/systemoptions \`
				` -H 'Content-Type: application/json' \`
				` -d '{`
				`  "instanceId": "e33ac015-081a-4e25-99c1-d1d6c332246e",`
				`  "cb_and_od_enabled": true,`
				`  "trafficPolicy": {`
				`  "connectionPool": {`
				`  "http": {`
				`  "http2MaxRequests": 1000`
				`  }`
				`  },`
				`  "outlierDetection": {`
				`  "consecutiveErrors": 5,`
				`  "interval": "10s",`
				`  "baseEjectionTime": "30s",`
				`  "maxEjectionPercent": 100`
				`  }`
				`  }`
				`  }'`

Table 3-9 (Cont.) Configuring Parameters for SystemOptions

Operation	Parameter	Value	Description	Example
	trafficPolicy.connectionPool.http.http2MaxRequests	Integer	Maximum number of requests to a backend. Default is 1024.	Set the value of **http2MaxRequests** field under **trafficPolicy.connectionPool.http** in the curl command. **http2MaxRequests UPDATE Command** `curl -X PUT \ http://<Soothsayerfqdn>:8081/soothsayer/v1/systemoptions \ -H 'Content-Type: application/json' \ -d '{ "instanceId": "e33ac015-081a-4e25-99c1-d1d6c332246e", "cb_and_od_enabled": true, "trafficPolicy": { "connectionPool": { "http": { "http2MaxRequests": 1000 } }, "outlierDetection": { "consecutiveErrors": 5, "interval": "10s", "baseEjectionTime": "30s", "maxEjectionPercent": 100 } } }'`

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 otherwise.

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.

- Error code to be sent if the Request cannot be alternate routed also on a per NF service basis.

Table 3-10 provides information about the configuring parameters for outlier detection.

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

Table 3-10 Outlier Detection Parameters

Parameter	Value	Description	Example

instanceId	String	Unique Id that represents systemOption record	Set the value of field **instanceId** in the curl command below:
			`curl -X PUT \`
			` http://<Soothsayerfqdn>:8081/soothsayer/v1/systemoptions \`
			` -H 'Content-Type: application/json' \`
			` -d '{`
			`  "instanceId": "e33ac015-081a-4e25-99c1-d1d6c332246e",`
			`  "cb_and_od_enabled": true,`
			`  "trafficPolicy": {`
			`  "connectionPool": {`
			`  "http": {`
			`  "http2MaxRequests": 1000`
			`  }`
			`  },`
			`  "outlierDetection": {`
			`  "consecutiveErrors": 5,`
			`  "interval": "10s",`
			`  "baseEjectionTime": "30s",`
			`  "maxEjectionPercent": 100`
			`  }`
			`  }`
			` }'`

Table 3-10 (Cont.) Outlier Detection Parameters

Parameter	Value	Description	Example
cb_and_od_enabled	Boolean	This tells whether Circuit-Breaking and Outlier-Detection is enabled or not.	Set the value of field **cb_and_od_enabled** in the curl command below: `curl -X PUT \ http://<Soothsayerfqdn>:8081/soothsayer/v1/systemoptions \ -H 'Content-Type: application/json' \ -d '{ "instanceId": "e33ac015-081a-4e25-99c1-d1d6c332246e", "cb_and_od_enabled": true, "trafficPolicy": { "connectionPool": { "http": { "http2MaxRequests": 1000 } }, "outlierDetection": { "consecutiveErrors": 5, "interval": "10s", "baseEjectionTime": "30s", "maxEjectionPercent": 100 } } }'`
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 '{ "instanceId": "e33ac015-081a-4e25-99c1-d1d6c332246e", "cb_and_od_enabled": true, "trafficPolicy": { "connectionPool": { "http": { "http2MaxRequests": 1000 } }, "outlierDetection": { "consecutiveErrors": 5, "interval": "10s", "baseEjectionTime": "30s", "maxEjectionPercent": 100 } } }'`

Table 3-10 (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 '{ "instanceId": "e33ac015-081a-4e25-99c1-d1d6c332246e", "cb_and_od_enabled": true, "trafficPolicy": { "connectionPool": { "http": { "http2MaxRequests": 1000 } }, "outlierDetection": { "consecutiveErrors": 5, "interval": "10s", "baseEjectionTime": "30s", "maxEjectionPercent": 100 } } }'`
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 '{ "instanceId": "e33ac015-081a-4e25-99c1-d1d6c332246e", "cb_and_od_enabled": true, "trafficPolicy": { "connectionPool": { "http": { "http2MaxRequests": 1000 } }, "outlierDetection": { "consecutiveErrors": 5, "interval": "10s", "baseEjectionTime": "30s", "maxEjectionPercent": 100 } } }'`

Table 3-10 (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 '{ "instanceId": "e33ac015-081a-4e25-99c1-d1d6c332246e", "cb_and_od_enabled": true, "trafficPolicy": { "connectionPool": { "http": { "http2MaxRequests": 1000 } }, "outlierDetection": { "consecutiveErrors": 5, "interval": "10s", "baseEjectionTime": "30s", "maxEjectionPercent": 100 } } }'`
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 '{ "instanceId": "e33ac015-081a-4e25-99c1-d1d6c332246e", "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/Deregister/Change notifications.

Parameters for Configuring NF Service Groups

Table 3-11 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 3-12 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.

Table 3-12 (Cont.) Supported Parameters

Query Parameter	Request Body	HTTP method or custom operation	Data type	P	Cardinality	Response Codes	Description
			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
			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`
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	PUT	NFServiceGroup	M	1	200 OK	Upon success, a response body is returned containing the updated NFServiceGroup object.
			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: Please refer to Data Model for Mandatory parameters.

Table 3-12 (Cont.) Supported Parameters

Query Parameter	Request Body	HTTP method or custom operation	Data type	P	Cardinality	Response Codes	Description
	the "Data Model" for this Request Body could be found in the "Data Models" section.		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 3-13 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.
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.
subsequentRequestRoutePolicy	SubReqRoutePolicy	M	This parameter can be modified.

SubReqRoutePolicy

Table 3-14 SubReqRoutePolicy

Field Name	Type	P	Description(With default Values)
routePolicy	Enum	M	Possible values: Forward_Proxy, Load_Balance
reroutePolicy	ReroutePolicy	M	

ReroutePolicy

Table 3-15 ReroutePolicy

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

NFServiceGroupModifiableFields

Table 3-16 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	
subsequentRequestRoutePolicy	SubReqRoutePolicy	O	

Configuring Operations for NF Service Groups

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

provides sample details of the operations to configure routing options.

Table 3-17 NF Service Groups Operations

Operations	REST Command

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

Table 3-17 (Cont.) NF Service Groups Operations

Operations	REST Command
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\"], \"subsequentRequestRoutePolicy\": { \"routePolicy\": \"Forward_Proxy\", \"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\"] }"

4
Metrics, KPIs, and Traces

This section provides the information for Metrics, KPIs, 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 4-1 Alert Reference

S.No	Alert Name	Severity	Comments
1	SCPIngressTrafficRateAboveMinorThreshold	Minor	Notify that Traffic rate is minor (user configure minor threshold value) with Locality and current value of traffic rate.
2	SCPIngressTrafficRateAboveMajorThreshold	Major	Notify that Traffic rate is major (user configure major threshold value) with Locality and current value of traffic rate.
3	SCPIngressTrafficRateAboveCriticalThreshold	Critical	Notify that Traffic rate is critical (user configure critical threshold value) with Locality and current value of traffic rate.
4	SCPRoutingFailedForServiceAlert	Minor	Notify that Routing failed for service. Provide details like NFService Type, NFType, Locality, and value.
5	SCPSoothsayerPodMemoryUsage	Warning	Notify Soothsayer per Pod memory usage is above threshold (here threshold value take n as 8 GB).
6	SCPWorkerPodMemoryUsage	Warning	Notify Worker per Pod memory usage is above threshold (here threshold value taken as 4 GB).
7	SCPPilotPodMemoryUsage	Warning	Notify Pilot per Pod memory usage is above threshold (here threshold value taken as 6 GB).

> **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 4-2:

Table 4-2 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`

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`

Table 4-2 (Cont.) Configuring Service Communication Proxy Alert in Prometheus

Step No.	Procedure	Description

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:
"{{$labels.ocscp_locality}}"  is above minor threshold (i.e. 1400 mps)'
          summary: 'Namespace: {{$labels.kubernetes_namespace}}, Pod:
{{$labels.kubernetes_pod_name}}: Current Ingress Traffic Rate is {{ $value |
printf "%.2f" }} mps which is above 70 Percent of Max MPS(2000)'
         # Provide app and kubernetes_namespace of scp deployed
        expr: sum(rate(ocscp_metric_total_http_rx_req{app="scp-
worker",kubernetes_namespace="scpsvc"}[2m])) by
(kubernetes_namespace,ocscp_locality,kubernetes_pod_name) >= 1400 < 1600
        labels:
```

```
          severity: Minor
      - alert: SCPIngressTrafficRateAboveMajorThreshold
        annotations:
          description: 'Ingress Traffic Rate at Locality:
{{$labels.ocscp_locality}} and is above major threshold (i.e. 1600 mps)'
          summary: 'Namespace: {{$labels.kubernetes_namespace}}, Pod:
{{$labels.kubernetes_pod_name}}: Current Ingress Traffic Rate is {{ $value |
printf "%.2f" }} mps which is above 80 Percent of Max MPS(2000)'
         # Provide app and kubernetes_namespace of scp deployed
        expr: sum(rate(ocscp_metric_total_http_rx_req{app="scp-
worker",kubernetes_namespace="scpsvc"}[2m])) by
(kubernetes_namespace,ocscp_locality,kubernetes_pod_name)  >= 1600 < 1800
        labels:
          severity: Major
      - alert: SCPIngressTrafficRateAboveCriticalThreshold
        annotations:
          description: 'Ingress Traffic Rate at Locality:
{{$labels.ocscp_locality}} and is above critical threshold (i.e. 1800 mps)'
          summary: 'Namespace: {{$labels.kubernetes_namespace}}, Pod:
{{$labels.kubernetes_pod_name}}: Current Ingress Traffic Rate is {{ $value |
printf "%.2f" }} mps which is above 95 Percent of Max MPS(1000)'
         # Provide app and kubernetes_namespace of scp deployed
        expr: sum(rate(ocscp_metric_total_http_rx_req{app="scp-
worker",kubernetes_namespace="scpsvc"}[2m])) by
(kubernetes_namespace,ocscp_locality,kubernetes_pod_name) >= 1800
        labels:
          severity: Critical
      - alert: SCPRoutingFailedForService
        annotations:
          description: 'Routing failed for service'
          summary: 'Routing failed for service: NFService Type =
"{{$labels.ocscp_nf_service_type}}", NFType = "{{$labels.ocscp_nf_type}}",
Locality = "{{$labels.ocscp_locality}}" and value = "{{ $value }}" '
         # Provide app and kubernetes_namespace of scp deployed
        expr: ocscp_metric_total_routing_send_fail{app="scp-
worker",kubernetes_namespace="scpsvc"}
        labels:
          severity: Minor
      - alert: SCPSoothsayerPodMemoryUsage
         # Provide kubernetes_namespace of scp deployed and pod name substring
as its regex match of pod name
        expr: sum(container_memory_usage_bytes{image!
="",namespace="scpsvc",pod_name=~".+soothsayer.+"})  by (pod_name, namespace,
instance) > 8589934592
        for: 2m
        labels:
          severity: Warning
        annotations:
          summary: "Instance: {{$labels.instance}}, NameSpace:
{{$labels.namespace}}, Pod: {{$labels.pod_name}}: Soothsayer Pod High Memory
usage detected"
          description: "Instance: {{$labels.instance}}, Namespace:
{{$labels.namespace}},Pod: {{$labels.pod_name}}: Memory usage is above 8G
(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!
="",namespace="scpsvc",pod_name=~".+worker.+"})  by (pod_name, namespace,
instance) > 4294967296
        for: 2m
```

```
        labels:
          severity: Warning
        annotations:
          summary: "Instance: {{$labels.instance}}, NameSpace:
{{$labels.namespace}}, Pod: {{$labels.pod_name}}: Worker Pod High Memory usage
detected"
          description: "Instance: {{$labels.instance}}, Namespace:
{{$labels.namespace}},Pod: {{$labels.pod_name}}: Memory usage is above 4G
(current value is: {{ $value }})"
      - alert: SCPPilotPodMemoryUsage
         # Provide kubernetes_namespace of scp deployed and pod name substring
as its regex match of pod name
        expr: sum(container_memory_usage_bytes{image!
="",namespace="scpsvc",pod_name=~".+pilot.+"})  by (pod_name, namespace,
instance)  > 6442450944
        for: 2m
        labels:
          severity: Warning
        annotations:
          summary: "Instance: {{$labels.instance}}, NameSpace:
{{$labels.namespace}}, Pod: {{$labels.pod_name}}: Pilot Pod High Memory usage
detected"
          description: "Instance: {{$labels.instance}}, Namespace:
{{$labels.namespace}},Pod: {{$labels.pod_name}}: Memory usage is above 6G
(current value is: {{ $value }})"
```

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>)"

Metrics Reference

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

Table 4-3 Metrics Reference

S.No	Promotheus Stat Metric Name	Metric Description	Dimensions	Example usage to filter metric by dimension on Grafana GUI	Metric Group
1	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"}	SCP Usage
2.	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"}	SCP Usage

Table 4-3 (Cont.) Metrics Reference

S.No	Promotheus Stat Metric Name	Metric Description	Dimensions	Example usage to filter metric by dimension on Grafana GUI	Metric Group
3	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"}	SCP Usage

Table 4-3 (Cont.) Metrics Reference

S.No	Promotheus Stat Metric Name	Metric Description	Dimensions	Example usage to filter metric by dimension on Grafana GUI	Metric Group
4	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"}	SCP Usage

Table 4-3 (Cont.) Metrics Reference

S.No	Promotheus Stat Metric Name	Metric Description	Dimensions	Example usage to filter metric by dimension on Grafana GUI	Metric Group
5	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{ocscp_response_code="201"} ocscp_metric_total_http_tx_res{ocscp_nf_type="UDM"} ocscp_metric_total_http_tx_res{ocscp_nf_service_type="nudm-uecm"} ocscp_metric_total_http_tx_res{ocscp_locality="Loc7"}	SCP Usage
6	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"}	SCP Usage
7	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"}	SCP Usage

Table 4-3 (Cont.) Metrics Reference

S.No	Promotheus Stat Metric Name	Metric Description	Dimensions	Example usage to filter metric by dimension on Grafana GUI	Metric Group
8	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"}	SCP Usage

Table 4-3 (Cont.) Metrics Reference

S.No	Promotheus Stat Metric Name	Metric Description	Dimensions	Example usage to filter metric by dimension on Grafana GUI	Metric Group
9	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"}	SCP Usage

Table 4-3 (Cont.) Metrics Reference

S.No	Promotheus Stat Metric Name	Metric Description	Dimensions	Example usage to filter metric by dimension on Grafana GUI	Metric Group
10	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"}	SCP Usage

Table 4-3 (Cont.) Metrics Reference

S.No	Promotheus Stat Metric Name	Metric Description	Dimensions	Example usage to filter metric by dimension on Grafana GUI	Metric Group
11	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"}	SCP Usage

Table 4-3 (Cont.) Metrics Reference

S.No	Promotheus Stat Metric Name	Metric Description	Dimensions	Example usage to filter metric by dimension on Grafana GUI	Metric Group
12	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"}	SCP Usage

Table 4-3 (Cont.) Metrics Reference

S.No	Promotheus Stat Metric Name	Metric Description	Dimensions	Example usage to filter metric by dimension on Grafana GUI	Metric Group
13	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 4-3 (Cont.) Metrics Reference

S.No	Promotheus Stat Metric Name	Metric Description	Dimensions	Example usage to filter metric by dimension on Grafana GUI	Metric Group
14	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 4-3 (Cont.) Metrics Reference

S.No	Promotheus Stat Metric Name	Metric Description	Dimensions	Example usage to filter metric by dimension on Grafana GUI	Metric Group
15	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 4-3 (Cont.) Metrics Reference

S.No	Promotheus Stat Metric Name	Metric Description	Dimensions	Example usage to filter metric by dimension on Grafana GUI	Metric Group
16	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"}	

Traces Reference

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

Table 4-4 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.
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.

Table 4-4 (Cont.) Traces Reference

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.
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

Table 4-4 (Cont.) Traces Reference

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.

HTTP status code supported on SBI

Table 4-5 HTTP status code supported on SBI

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

Table 4-5 (Cont.) HTTP status code supported on SBI

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	
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

Table 4-5 (Cont.) HTTP status code supported on SBI

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	

Table 4-5 (Cont.) HTTP status code supported on SBI

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")

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.

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 4-6 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)
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.

Table 4-6 (Cont.) Protocol and application errors

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.