# Oracle® Communications Network Analytics Data Director Outbound Interface Specification Guide





Oracle Communications Network Analytics Data Director Outbound Interface Specification Guide,

F86972-02

Copyright © 2023, 2024, Oracle and/or its affiliates.

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

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

If this is software, software documentation, data (as defined in the Federal Acquisition Regulation), or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

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

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

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

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

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

# Contents

L Int	roduction	
1.1 1.2		1
2 Are	chitecture	
3 Da	ata Director Configuration	
3.1	Requirements	1
3.2		1
	<ul><li>3.2.1 Metadata</li><li>3.2.2 Data Director Message</li></ul>	2
	3.2.2 Data Director Message 3.2.2.1 Data Director Message Format	: :
	3.2.2.2 Third-Party Feed Format	6
	3.2.2.3 Example for the JSON Data	6
3.3	xDR	7
	3.3.1 xDR Format	7
Th	aird-party Tool Configuration	
4.1	For HTTP2 and Synthetic TCP Feed	1
	4.1.1 Multiple IP Addresses	1
4.2	For Kafka Consumer Feed	1
Da	ata Stream Contents	
5.1	Traffic Feed Contents	
5.2	xDR Contents	3
Hi	gh Availability for Feed	

# Error Handling

7

# My Oracle Support (MOS)

My Oracle Support (<a href="https://support.oracle.com">https://support.oracle.com</a>) 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 <a href="http://www.oracle.com/us/support/contact/index.html">http://www.oracle.com/us/support/contact/index.html</a>. When calling, make the selections in the sequence shown below on the Support telephone menu:

- 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.
- For Hardware, Networking and Solaris Operating System Support, select 3.

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.

# Acronyms

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

### Table Acronyms

Acronym	Description		
3GPP	3rd Generation Partnership Project		
	3GPP is the standard body for wireless communications		
NWDAF	Oracle Communications Networks Data Analytics Function		
5G	Fifth Generation		
	5G is the fifth-generation technology standard for broadband cellular networks		
ACL	Access Control List		
CNC	Cloud Native Core		
	CNC is a market-leading core network solution utilizing Cloud Native principles and architecture to deliver Service Agility, Innovation, Efficiency, and Adaptability for 4G and 5G network functions including an optional on-premises Cloud Native Environment		
C-NF	Consumer Network Function		
CSP	Communication Service Provider		
HA	High Availability		
	High-availability infrastructure is configured to deliver quality performance and handle different loads and failures with minimal or zero downtime		
НТТР	Hypertext Transfer Protocol		
	HTTP is an application-layer protocol for transmitting hypermedia documents, such as HTML. It was designed for communication between web browsers and web servers, but it can also be used for other purposes		
HTTP2	Hypertext Transfer Protocol version 2		
	HTTP2 is a major revision of the HTTP network protocol used by the World Wide Web		
JSON	Java Script Object Notation		
	JSON is a language-independent, text-based data format that can represent objects, arrays, and scalar data		
mTLS	Mutual Transport Layer Security		
	mTLS authentication ensures that traffic is both secure and trusted in both directions between a client and server. It allows requests that do not log in with an identity provider (like IoT devices) to demonstrate that they can reach a given resource		
MVP	Minimum Viable Product		
NF	Network Function		



# Table (Cont.) Acronyms

Acronym	Description		
NRF	Network Repository Function or Network Function Repository Function		
	NRF is a key component of the 5G Service Based Architecture. It maintains an updated repository of all the NFs available in the operator's network along with the services provided by each of the NFs in the 5G core that is expected to be instantiated, scaled, and terminated with minimal to no manual intervention		
P-NF	Producer Network Function		
SBI	Service Based Interface		
	SBI is the term given to the API based communication that can take place between two NFs		
SCP	Service Communication Proxy		
	SCP helps operators to efficiently secure and manage their 5G network by providing routing control, resiliency, and observability to the core network. It leverages IT service mesh (ISTIO) and adds critical capabilities to make it 5G-aware, thereby addressing many of the challenges caused by the new service-based architecture (SBA) in the 5G core		
SEPP	Security Edge Protection Proxy		
	SEPP as a 5G node is a non-transparent proxy that sits at the perimeter of the Public Land Mobile Network (PLMN) network and enables secured communication between inter-PLMN network messages. It is a Cloud native solution based on microservice architecture which acts as a non-transparent proxy sitting at the perimeter of the PLMN network enabling secured inter NF communication across PLMN networks		
TCP	Transmission Control Protocol		
	TCP is a connection-oriented protocol used by applications on networked hosts to connect to one another and to exchange streams of data in a reliable and in-order manner		
TLS	Transport Layer Security		
	TLS and its now-deprecated predecessor, Secure Sockets Layer, are cryptographic protocols designed to provide communications security over a computer network		

# What's New in This Guide

This section introduces the documentation updates for Release 23.4.x in Oracle Communications Network Analytics Data Director Outbound Interface Specification Guide.

## Release 23.4.0.0.1 - F86972-02, July 2024

There are no updates to this document in this release.

### Release 23.4.0 - F86972-01, December 2023

- Updated <u>Architecture</u> with the details of the following features:
  - Correlation and xDR
  - Synthetic Packet Generation
  - Data Director Network Visibility & KPIs
- Updated <u>Requirements</u> details
- Added the details of <u>xDR</u> and <u>xDR Format</u>.
- Updated <u>Third-party Tool Configuration</u> details.
- Updated <u>Data Stream Contents</u>.

# Introduction

This document provides information on the Data Director Outbound Interface specifications required by customers to use Oracle's SBI Application-Level Traffic Feed solution.

# 1.1 Overview

5G SBI Application-Level Traffic Feed Solution is a common pre-integrated, on demand, and automated solution that is applicable across all NFs, independent of the underlying infrastructure to mirror the 5G SBI message flows towards analytics or third-party tools.

The solution has no specific dependencies, but it provides clear insights into direct NF-to-NF communications. In addition, it maintains security while mirroring the required data and provides all necessary data through standardized interfaces to third-party consumers.

# 1.2 References

For more information on OCNADD, refer to the following documents:

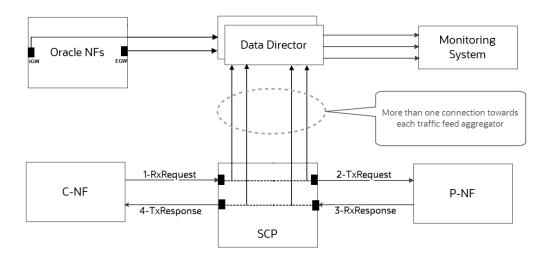
- Oracle Communications Network Analytics Data Director User Guide
- Oracle Communications Network Analytics Data Director Troubleshooting Guide
- Oracle Communications Network Analytics Data Director Installation, Upgrade, and Fault Recovery Guide
- Oracle Communications Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide
- Oracle Communications Cloud Native Core cnDBTier Installation, Upgrade, and Fault Recovery Guide
- Oracle Communications Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide
- Oracle Communications Network Analytics Suite Security Guide
- Oracle Communications Network Analytics Data Director Benchmarking Guide

# **Architecture**

This chapter covers the Oracle's 5G SBI Application-Level Traffic Feed solution that demonstrates SBI traffic feed going from Oracle 5G NFs to Oracle Data Director (acting as a traffic feed aggregator).

Following is a high-level block diagram showing the traffic feed from Oracle NFs:

Figure 2-1 Traffic Feed from Oracle NFs

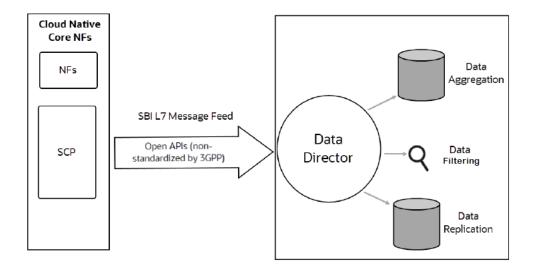


The message mirroring takes place through four endpoints covering RxRequest, TxRequest, RxResponse, and TxResponse with respect to SCP and through two endpoints. namely, Ingress and Egress Gateways with respect to Oracle NFs. All transactions are mirrored for both SCP and Oracle NFs.

Following is a high-level block diagram depicting the solution overview:



Figure 2-2 Solution Overview



Data Director is a solution within the Network Analytics suite, which addresses the 5G traffic feed aggregation and data enrichment. It assimilates the data required to statistical prediction.

Data Director provides the following key features:

### Correlation and xDR

- Correlation feature generates xDRs from network transactions, enabling insights.
- xDRs aid in network troubleshooting, tracing scenarios across NFs, and KPI generation.
- Enhances network visibility and observability through KPIs and threshold alerts.
- Enables network efficiency reports via intuitive dashboards.
- xDRs facilitate advanced descriptive and predictive network analytics.
- Supports integration with network analytics frameworks like NWDAF or Insight Engine.

### Aggregation

- Collects and aggregates the network traffic from multiple NFs, for example, SCP, SEPP, and NRF.
- Provides the aggregated traffic feed to one or many third-party monitoring tools.

### Filtering

- Filtering is supported for selected metadata and header attributes in OCNADD.
- Delivers only relevant traffic, such as traffic matching specific consumer-id and/or service-name, to the third party tool.
   For more information, see "Data Filtering" and "Data Filters List" sections in *Oracle Communications Network Analytics Data Director User Guide*.

### Replication

- Feeds multiple third-party systems with the collected feed, for example, to the monitoring, troubleshooting, and security tool.
- Secure Transport (TLS)



- Provides the data delivery to third-party tools securely.
- Synthetic Packet Generation
  - Synthetic packet generation in Data Director converts incoming JSON data to network transfer wire format.
  - Supports L3L4 mapping on DD that allows end user to map L3 and L4 information with desired metadata/L7 layer parameters
  - Transfers converted packets securely to 3rd party monitoring probes.
  - Third party probes utilize these synthetic packets for internal monitoring applications.
  - Eliminates the necessity for additional applications by vendors to handle JSON data.
  - Saves critical compute resources and reduces associated costs for vendors.
- High Availability
  - Data Director is implemented as a Kubernetes service.
  - Multiple Kafka connections from NFs and Data Director are established to stream the ingress data from NFs.
  - Each instance of the Data Director supports two HTTP2 endpoints of the third-party monitoring tools.
  - The number of connections depends on the amount of throughput required.
- Data Director Network Visibility & KPIs
  - Data Director as a data broker holds network data for generating reports and KPIs.
  - Reports and KPIs via dashboards offer insights and operational support.
  - Generates KPIs for network utilization and load, enhancing visibility.
  - xDRs from correlated messages used for intuitive network efficiency reports.

# **Data Director Configuration**

This chapter lists the Data Director Configuration requirements on Oracle Communications Cloud Native Environment.

# 3.1 Requirements

Before you begin with the procedure for setting up Data Director in Cloud Native Core, ensure that the following requirements are met:

- The metadata from NFs
- The third-party target that receives the packets
- Optional TLS config for For HTTP2 and Synthetic TCP Feeds
- The HTTP standards require a response for every message sent. Oracle will provide a configuration option to ignore the response for HTTP2 Feed.
- The message acquisition point is configurable (ingress or egreess, or both) at the NF level.
- Kafka consumer Feed is enabled only when OCNADD services are on TLS.
- Create ACL user prior to creating Kafka feeds.

### (i) Note

With the HTTP2 ignore the response option enabled the OCNADD considers message transfer as successful as soon as data is sent to 3rd party monitoring consumers. OCNADD does not wait for 200 OK response to consider the message transfer as successful. Message retransmission is not attempted. However, for maintaining the connection status to 3rd party monitoring App endpoints, OCNADD still expects response for each post request sent to 3rd party monitoring App.

# 3.2 Outbound Protocols

Data Director currently supports three Egress Feed types, over which the 5G SBI messages and metadata added by the NFs are forwarded to third-party consumers:

- HTTP2 Feed: The HTTP2 Feed is used for monitoring purposes. It employs the HTTP/2 protocol, utilizing JSON as the application layer serialization protocol. Additionally, there is an option to implement TLS for security protection at the transport layer.
- Synthetic Feed: The Synthetic Feed operates through a TCP connection, enabling the
  transmission of synthetic packets. These packets contain comprehensive L2 to L7
  information, complete with synthesized layers and necessary information. For added
  security at the transport layer, optional TLS is available.
- Kafka Consumer Feed: The Kafka Consumer Feed allows 3rd-party consumers to retrieve the 5G SBI messages and metadata introduced by the NFs in the form of JSON



documents, using the Kafka consumer API. To enhance security during transmission, TLS is employed at the transport layer.

# 3.2.1 Metadata

The following table lists the components that are part of the available metadata from SCP:



### Note

For more information on each metadata component, see <u>Data Stream Contents</u>.

Table 3-1 Format based on 3GPP

Metadata	Information		
	This is a unique identifier in the message for correlation within a single transaction.		
correlation-id	<ul> <li>If an intermediate Oracle NF like SCP or SEPP sees a correlation-id custom header in the message, then it forwards the header without any modification.</li> <li>Oracle NFs add the correlation-id custom header in the responses.</li> </ul>		
	This is a 5G NF Instance ID of the NF originating the received message.		
consumer-id	<ul> <li>Depends on the presence of the User-Agent header in the received service request</li> <li>Recommended User-Agent header format: User-Agent:<nf type="">-<nf id="" instance=""> <nf FQDN&gt;</nf </nf></nf></li> </ul>		
producer-id	<ul> <li>This is a 5G NF Instance ID of the destination NF.</li> <li>Oracle SCP can find the destination NF instance Id using the authority in the service request and learning from the NRF.</li> <li>Other Oracle NFs may not be able to find NF instance id of destination in be able to put destination FQDN</li> </ul>		
consumer-fqdn	This is a FQDN of the network function originating the received message.  Depends on the presence of User-Agent header in the received service request  Recommended User-Agent header format: User-Agent: <nf type="">-<nf id="" instance=""> <ni fqdn=""></ni></nf></nf>		
producer-fqdn	This is an FQDN of the destination NF. It depends on the presence of FQDN in the authority of service request.		
hop-by-hop-id	Oracle NFs can add Hop-by-Hop id to identify a request and response pair to the next node. This is required in addition to correlation-id for uniquely identifying the request-response pair in case of rerouting.		



Table 3-1 (Cont.) Format based on 3GPP

Metadata	Information		
reroute-cause	<ul> <li>Indicate the re-route cause. Contains one of the following:</li> <li>Circuit breaking: Flag to indicate that a message is an alternate attempt due to circuit breaking functionality at the SCP</li> <li>Outlier detection: Flag to indicate that a message is an alternate attempt due to outlier detection functionality at the SCP</li> <li>Egress-rate-limit: Flag to indicate that a message is an alternate attempt due to egress rate limiting functionality at the SCP</li> <li>producer-nf-congestion: Flag to indicate that a message is an alternate attempt due to producer NF congestion</li> <li>Error received</li> <li>Timeout</li> <li>Not Available</li> </ul>		
timestamp	This is a timestamp (in nanoseconds) at the traffic feed trigger point when the message is received or forwarded by the SCP. It is an epoch time.		
message-direction	This is a parameter to indicate whether a message is ingress to or egress from NF. It can be indicated by putting the traffic feed trigger point name.  RxRequest TxRequest RxResponse TxResponse		
feed-source	Source of this traffic feed. This contains the key- value of different identity of the node sending the traffic feed.  • Feed-source:  - nf-type = SCP  - nf-fqdn = SCP's FQDN  - nf-instance-id = SCP's NF instance id  - pod-instance-id = SCP-worker's pod instance id		

# 3.2.2 Data Director Message

The 5G SBI message that is received or forwarded contains the following components:

- HTTP2: HTTP2 Headers All received HTTP2 standard and 3gpp defined headers.
- Received Data Director Message Payload

# 3.2.2.1 Data Director Message Format

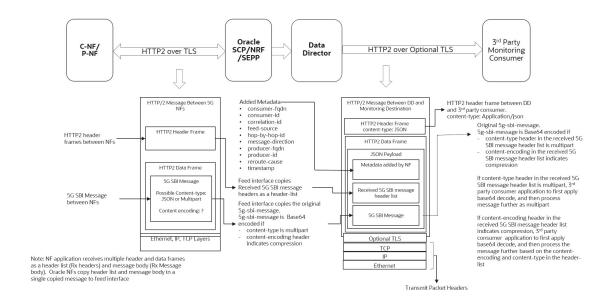
The Data Director supports the following message formats:

- HTTP2 Message Format
- Synthetic Packet Message Format



Kafka Consumer Egress Feed Message Format

### **HTTP2 Message Format**



Data Director supports HTTP2 feed for forwarding from Data Director to third-party monitoring consumer applications. 5G monitoring data is forwarded to third-party monitoring consumer using HTTP2 POST requests. The following components are delivered as JSON payload in the HTTP2 data frames:

- Original received 5G SBI message headers as a header-list.
- Original received 5g sbi data as 5g-sbi-message
- · Metadata-list added by NF

The 5g-sbi-message forwarded to third-party consumer application is Base64 encoded if:

The content-type header in the received 5G SBI message header list is multipart

Or

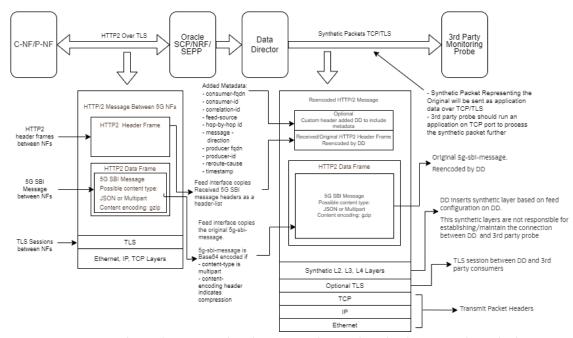
The content-encoding in the received 5G SBI message header list indicates compression

If the "content-type" header in the received 5G SBI message header list is labeled as "multipart," the third-party consumer application performs an initial base64 decode. Subsequently, the application proceeds to process the message as multipart content.

When the "content-encoding" header in the received 5G SBI message header list shows compression, the third-party consumer application first applies base64 decode. Then, it processes the message further based on the content-encoding and content-type in the header list.

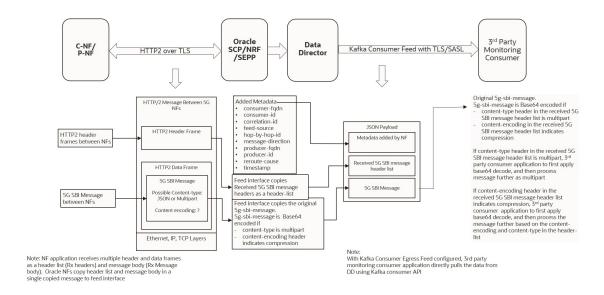
### **Synthetic Packet Message Format**





OCNADD converts incoming JSON data into network transfer wire format and sends the converted packets to the third-party monitoring applications in a secure manner. The third-party probe feeds the synthetic packets to the internal monitoring applications. The feature helps third-party vendors to eliminate the need of creating additional applications to receive JSON data and converting the data into probe compatible format, thereby saving critical compute resources and associated costs.

# Kafka Consumer Egress Feed Message Format



OCNADD supports the external Kafka consumer applications using the external Kafka Feeds. This enables third-party consumer applications to directly consume data from the Data Director Kafka topic, eliminating the need for any egress adapter.

Clients need to be authenticated through either SASL or SSL (mTLS) for authorization by Kafka. As a result, enabling external Kafka feed support requires specific settings to be activated within the Kafka broker. This ensures mandatory authentication of Kafka clients by the Kafka service.



OCNADD only allows authorized and authenticated third-party applications to use the Data Director Kafka service. Application authorization is handled using the KAFKA ACL (Access Control List) functionality. Access control for the external feed is established during Kafka feed creation. Presently, third-party applications are exclusively allowed to READ from a specific topic using a designated consumer group.

# 3.2.2.2 Third-Party Feed Format

### **Third-Party HTTP2 Feed Format**

A third-party HTTP2 feed contains the following components:

Figure 3-1 Third-Party HTTP2 Feed Format

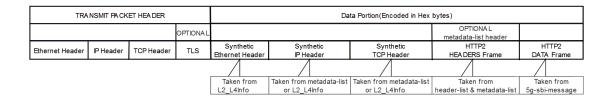
Transmit Packet Header			Data Portion			
		Optional		JSON		
IPv4 Header	TCP Header	TLS	HTTP/2 Hdr	Mirror 5G SBI Message	Received 5G SBI Message Headers	Metadata Added by Mirror Feed Source

Following TLS options are supported:

- TLSv1.2 (minimum) with oracle approved TLS Ciphers
- TLSv1.2 with Static Key Cipher support (TLS RSA WITH AES 128 GCM SHA256)
- No TLS (H2C)

### **Third-Party Synthetic Feed Format**

A third-party synthetic feed contains the following components:



# 3.2.2.3 Example for the JSON Data



For more information on the metadata list, see Metadata.



Following is an example for the JSON data:

```
{
    "version": "Major.Minor.Patch",
    "metadata-list":{},
    "header-list":{
        ":authority":"10.75.224.64:30065",
        ":method": "PUT",
        ":path":"/USEast/nudm-uecm/v1/imsi-5566700000000/registrations/
amf-3qpp-access",
        ":scheme": "http",
        "content-type": "application/json",
        "3qpp-sbi-target-apiroot": "http://
udm1svc.default.svc.cluster.local:8080/USEast",
        "3qpp-sbi-message-priority": "5",
        "content-length": "501",
        "accept-encoding": "gzip",
        "user-agent": "Go-http-client/2.0"
    },
    "5g-sbi-message":{
        "quami":{
            "plmnId":{
                "mcc": "233",
                "mnc": "23"
            "amfId": "100000"
        },
        "pei": "imei-456565651000000",
        "attrib1": "abcdefghijklmnopqurestuvwxqweoeqwowertyo123445678",
        "attrib2": "abcdefghijklmnopqurestuvwxqweoeqwowertyo123445678",
        "attrib3": "abcdefghijklmnopqurestuvwxqweoeqwowertyo123445678",
        "attrib4": "abcdefqhijklmnopqurestuvwxqweoeqwowertyo432123445678",
        "attrib5": "abcdefqhijklmnopqurestuvwxqweoeqwowert234yo123445678",
        "pcscfRestorationCallbackUri": "http://pcf1.pcf1svc.svc.cluster.local/
notification/udmtest"
```

# 3.3 xDR

xDRs generated by correlation services are stored in corresponding xDR topic as JSON data. External application acting as Kafka consumer can subscribe to the xDR Kafka topic to read the xDR data. For more information on mandatory and optional xRD contents, see *Oracle Communications Network Analytics Data Director User Guide*.

# 3.3.1 xDR Format

Following is an example for xDR when includeMessageWithxDR option is set to none.



```
"configurationName": "corr-test-2",
    "xdrStatus": "SUDR",
    "path": "/nudm-uecm/v1/imsi-208014489186000/registrations/smf-
registrations/1",
    "supi": "imsi-208014489186000",
    "methodType": "PUT",
    "producerNfType": "SCP",
    "consumerFqdn": "SMF.5g.oracle.com",
    "producerFqdn": "UDM.5g.oracle.com",
    "contentType": "application/json",
    "ueId": "imsi-208014489186000",
    "pduSessionId": 1,
    "smfInstanceId": "8e81-4010-a4a0-30324ce870b2",
    "snssai": "{\u0022sst\u0022:1,\u0022sd\u0022:\u0022000001\u0022}",
    "pcfInstanceId": "8e81-4010-a4a0-30324823334"
]
```

# (i) Note

includeMessageWithxDR option allows user to select whether original feed message will be included with xDR or not and If included, which part of message to be included.

### Below examples capture xDRs with includeMessageWithxDR

includeMessageWithxDR is set to DATA

```
// XDR
    "version": "1.0.0",
    "configurationName": "cap4c",
    "beginTime": "2023-06-26T14:40:29.950313200",
    "endTime": "2023-06-26T14:40:29.950313200",
    "xdrStatus": "SUDR",
},
// MESSAGE 1
    "5g-sbi-message":
       No change in data(
            if incoming data to DD is nested, same will be transferred)
},
// END OF MESSAGE 1
// MESSAGE 2
    "5g-sbi-message":
       No change in data(
            if incoming data to DD is nested, same will be transferred)
}
```



• includeMessageWithxDR is set to HEADERS\_DATA

includeMessageWithxDR is set to METADATA\_HEADERS\_DATA

```
// XDR
   "version": "1.0.0",
   "configurationName" : "cap4c",
   "beginTime" : "2023-06-26T14:40:29.950313200",
   "endTime" : "2023-06-26T14:40:29.950313200",
   "xdrStatus" : "SUDR",
 },
 // MESSAGE1
   "metadata-list":{No change in format},
   "header-list": {No change in format},
   "5g-sbi-message":{No change in format}
 // END OF MESSAGE 1
 // MESSAGE2
   "metadata-list":{No change in format},
   "header-list":{No change in format},
   "5g-sbi-message":{No change in format}
```



// END OF MESSAGE 2



The format of message would be same that is received in OCNADD from Oracle NFs.

# **Third-party Tool Configuration**

Customers need to configure respective HTTP2 endpoints of third-party tools in Data Director. The connection status is managed at the TCP stack level.

# 4.1 For HTTP2 and Synthetic TCP Feed

Customers need to configure respective HTTP2/TCP endpoints of third-party tools in Data Director. The connection status is managed at the TCP stack level. For more information, see *Oracle Communications Network Analytics Data Director User Guide*.

# 4.1.1 Multiple IP Addresses

Each instance of the Data Director supports two HTTP2/TCP endpoints of the third-party monitoring tools.

# 4.2 For Kafka Consumer Feed

Customers need to configure ACL User for Kafka feed on Data Director to authorize the third-party application. Then the Kafka consumer on external application can be configured to subscribe to respective Kafka topic and stream data. For more information, see *Oracle Communications Network Analytics Data Director User Guide* 

# **Data Stream Contents**

# 5.1 Traffic Feed Contents

The 5G SBI feed message that is forwarded third-party contains the following components:

- Received 5G SBI Message Headers.
- Received 5G SBI Message Body
- Metadata added by traffic feed.

Following are the metadata added by traffic feed:

### correlation-id

This is a unique identifier in the message for correlation within a single transaction.

- If an intermediate Oracle NF like SCP or SEPP sees a correlation-id custom header in the message, then it forwards the header without any modification.
- Oracle NFs add the correlation-id custom header in the responses.

The actual correlation-id custom header name is confirmed during the implementation.

### consumer-id

This is a 5G NF Instance ID of the NF originating the received message.

- Depends on the presence of the User-Agent header in the received service request
- Recommended User-Agent header format: User-Agent:<NF Type>-<NF Instance ID> <NF FQDN>

### producer-id

This is a 5G NF Instance ID of the destination NF.

- Oracle SCP can find the destination NF instance Id using the authority in the service request and learning from the NRF.
- Other Oracle NFs may not be able to find NF instance id of destination in be able to put destination FQDN.

### consumer-fqdn

This is a FQDN of the network function originating the received message.

- Depends on the presence of User-Agent header in the received service request
- Recommended User-Agent header format: User-Agent:<NF Type>-<NF Instance ID> <NF FQDN>

### producer-fqdn

This is an FQDN of the destination NF.



Depends on the presence of FQDN in the authority of service request.

### hop-by-hop-id

Oracle NFs can add Hop-by-Hop id to identify a request and response pair to the next node.

This is required in addition to correlation-id for uniquely identifying the request-response pair in case of re-routing.

### re-route cause

Indicates the re-route cause. Contains one of the following:

- Circuit breaking: Flag to indicate that a message is an alternate attempt due to circuit breaking functionality at the SCP.
- Outlier detection: Flag to indicate that a message is an alternate attempt due to outlier detection functionality at the SCP.
- Egress-rate-limit: Flag to indicate that a message is an alternate attempt due to egress rate limiting functionality at the SCP.
- producer-nf-congestion: Flag to indicate that a message is an alternate attempt due to producer NF congestion.
- Error received
- Timeout
- Not Available

### timestamp

This is a timestamp (in nanoseconds) at the traffic feed trigger point when the message is received or forwarded by the SCP. It is an epoch time.

### message-direction

This is a parameter to indicate whether a message is ingress to or egress from NF.

It can be indicated by putting the traffic feed trigger point name.

- RxRequest
- TxRequest
- RxResponse
- TxResponse

### feed-source

Source of this traffic feed. This contains the identity of the node sending the traffic feed.

### Feed-source:

- nf-type = NF Type
- nf-fqdn = NF's FQDN
- nf-instance-id = NF instance id
- pod-instance-id = pod instance id

Data Director makes reasonable attempts to deliver packets in the same sequence as received from each pod (SCP Worker pod, NRF, or SEPP API GW pod).



Due to the parallel nature of sending packets across multiple pods within CNE and IP routing, reception in order at the monitoring system cannot be guaranteed. Note that within a single transaction, request and answer follow the same path and processed by the same pod, therefore, there is no need to follow the packet order across multiple pods.

# 5.2 xDR Contents

For details on mandatory and optional xDR content, see *Oracle Communications Network Analytics Data Director User Guide*.

# High Availability for Feed

Data Director will support High Availability as per the requirements of customers.

Messages will be available for up to six hours in case of site connectivity issues. Increased redundancy or message caching will require additional resources. Customers will be provided with an option to configure the message caching for up to six hours.



### (i) Note

Current Data Director software release assumes underlying data storage provides data redundancy.

In case of recovery after failure, the data streaming will resume from where it got stopped. If the failure duration is more than the retention duration (based on the HA configuration), the streaming will resume from the oldest available data stored in Data Director.

# **Error Handling**

The error handling is maintained by 5G Core NFs. Data Director is an aggregator of 5G Core NF Feed and streams it towards the third-party tools. However, Data Director can create more than one copy of messages, so the message loss is mitigated. Also, Data Director caches the messages for up to six hours and restarts the stream once connectivity is restored with the third-party system.

### (i) Note

Current Data Director software release assumes underlying data storage provides data redundancy.