Oracle® Communications

Network Analytics Data Director Diameter User Guide

Release 25.2.200

G48765-01

December 2025

Oracle Communications Network Analytics Data Director Diameter User Guide, Release 25.2.200

G48765-01

Contents

1 Introduction

2 OCNADD Architecture

3 OCNADD Features and Feature Specific Limits

4 User Interface

5 Parameter Update in OCNADD Microservices

6 Kafka & Communication Management

7 Metrics, KPIs, Alerts, and Alarms

Preface

- Documentation Accessibility
- Diversity and Inclusion
- Conventions

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customer access to and use of Oracle support services will be pursuant to the terms and conditions specified in their Oracle order for the applicable services.

Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

My Oracle Support (MOS)

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:

- 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
ACL	Access Control List
AF	Application Function
API	Application Programming Interface
CNC	Cloud Native Core
CNC Console	Cloud Native Configuration Console
CNE	Oracle Communications Cloud Native Core, Cloud Native Environment
CNLB	Cloud Native Load Balancer
FQDN	Fully Qualified Domain Name
GUI	Graphical User Interface
HA	High Availability
HTTPS	Hypertext Transfer Protocol Secure
K8s	Kubernetes
KPI	Key Performance Indicator
ME	Monitoring Events
ML	Machine Learning
NF	Network Function
OAM	Operations, Administration, and Maintenance
OCI	Oracle Cloud Infrastructure
OCNADD	Oracle Communications Network Analytics Data Director
REST	Representational State Transfer
SBA	Service Based Architecture
SBI	Service Based Interface
SMF	Session Management Function
SNMP	Simple Network Management Protocol
SSL	Secure Sockets Layer
SUPI	Subscription Permanent Identifier
TLS	Transport Layer Security
UE	User Equipment
URI	Uniform Resource Identifier

What's New in This Guide

This section introduces the documentation updates for Release *25.2.2xx* in *Oracle Communications Network Analytics Data Director Diameter User Guide*.

Release 25.2.200 - G48765-01, December 2025

This is the initial release of this document.

1 Introduction

This document provides information about the role of Oracle Communications Network Analytics Data Director (OCNADD) in the Network Analytics suite of products, as well as instructions on how to configure and use OCNADD services and managed objects.

1.1 Overview

OCNADD is a specialized Network Data Broker (NDB) in 5G and Diameter Network Architecture.

OCNADD receives network traffic data from various sources: 5G network functions (NFs), non-5G NFs, and Diameter nodes. It performs replication and aggregation on the received data according to rules implemented by the subscribed third-party consumers. OCNADD sends the replicated and aggregated data to the subscribed third-party consumer applications or platforms in a secure manner.

OCNADD ensures data security, low latency, and redundancy while collecting and processing data. It enables Communication Service Providers (CSPs) to correlate and transform the acquired data as per their data feed configuration to create comprehensive dashboards and Key Performance Indicators (KPIs), thereby achieving meaningful insights about all functions in 5G Network Architecture. This information can be used for monetizing, providing good quality of service, reducing downtime, easing network scalability, and minimizing losses. The OCNADD-generated data can be beneficial for monitoring and troubleshooting issues during a network failure.

OCNADD performs the following key functions:

- **Data aggregation:** Collects and aggregates network traffic data from Diameter nodes, such as vDSR, and multiple NFs including SCP, SEPP, PCF, BSF, and NRF. The NFs can be located at a single site or across different sites. OCNADD routes the consolidated traffic data to third-party consumer applications or monitoring tools that have subscribed to receive the traffic data.
- **Data replication:** Routes the consolidated data to multiple third-party consumer applications that use the data for monitoring, troubleshooting, or security purposes. Multiple data feeds are received based on the filtering configurations specified by the third-party consumer applications. OCNADD replicates these feeds to more than one third-party consumer application. It also provides the feed to multiple third-party systems, such as monitoring, troubleshooting, and security tools, with the collected data.

  > ⓘ **Note**
  >
  > OCNADD supports replication for a maximum of two third-party consumer applications.

- **Synthetic Packet Data Generation:** Enables OCNADD to convert incoming JSON data into network transfer wire format and send the converted packets securely to third-party monitoring probes. The third-party probe feeds the synthetic packets to the internal monitoring applications. This feature helps third-party vendors eliminate the need to create additional applications for receiving JSON data and converting it into a probe-compatible format, thereby saving critical compute resources and associated costs.

- **Secure data transport (TLS):** Provides secure data communication between producer NFs and third-party consumer applications. Both the incoming data streaming towards OCNADD and the outgoing data streaming towards third-party applications are TLS encrypted.
- **Operational dashboard:** Provides a dashboard with various visualization operations and a panel for configuring metrics, KPIs, and monitoring alarms to track the system's health.
- **Data governance:** Supports data governance by managing the availability, usability, integrity, and security of data in enterprise systems based on Oracle data standards and policies that control data usage.
- **Health monitoring:** Includes a health monitoring functionality to monitor the readiness and liveliness of each microservice instance. The health monitoring feature also provides health reports for each OCNADD service, which can be monitored on demand or periodically using the OCNADD dashboard.
- **Backup and restore:** Provides backup and restore functionality to enable high availability and quick recovery from any failures. Configuration backups are taken periodically from the deployed setup so that, if a cluster fails, it can be restored quickly.
- **High availability:** The OCNADD instance is deployed in pods within Kubernetes clusters, ensuring high availability of the services. In case of a failure, a new instance of the services is immediately available. If a Kubernetes cluster fails, the OCNADD deployment is restored to a different cluster.
- **Message sequencing:** Provides sequenced message delivery to third-party applications with configuration options (TIME_WINDOW, REQUEST_RESPONSE, and TRANSACTION).

> ⓘ **Note**
>
> A maximum of two data feeds is recommended if a higher MPS rate is required (e.g., the same as the ingress MPS rate). Additionally, it must be noted that replicated feeds are supported up to a 135 K MPS ingress rate.

1.2 References

Refer to the following documents for more information:

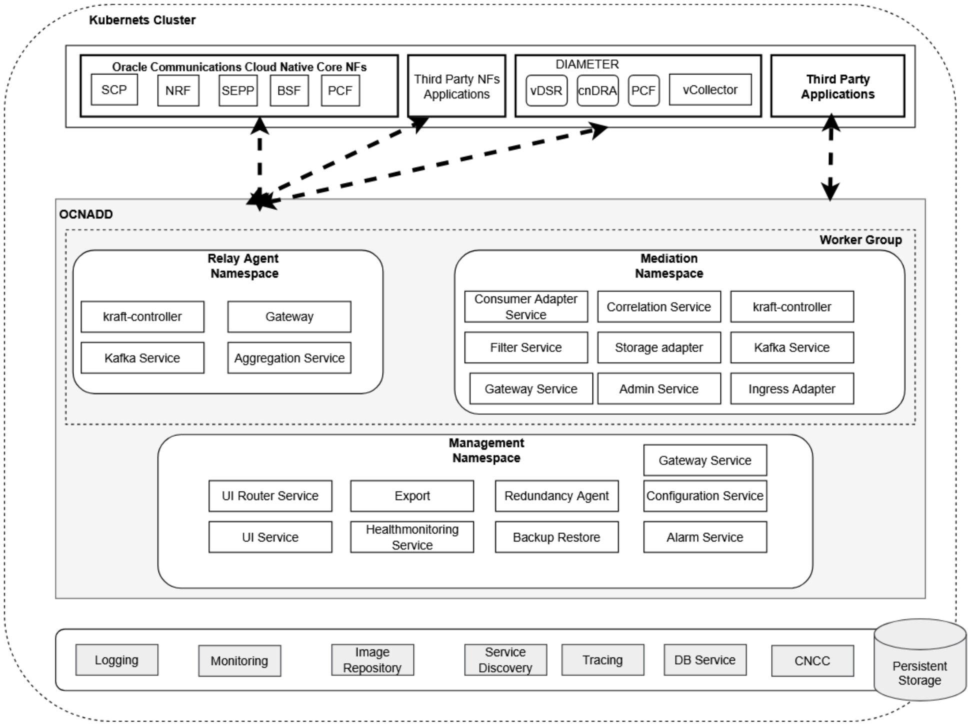
- *Oracle Communications Network Analytics Data Director User Guide*
- *Oracle Communications Network Analytics Data Director Installation, Upgrade, and Fault Recovery Guide*
- *Oracle Communications Network Analytics Data Director Troubleshooting Guide*
- *Oracle Communications Network Analytics Data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

2 OCNADD Architecture

This chapter outlines the architectural principles and deployment structure of OCNADD.

Figure 2-1 OCNADD Architecture



2.1 OCNADD Centralized Deployment Architecture

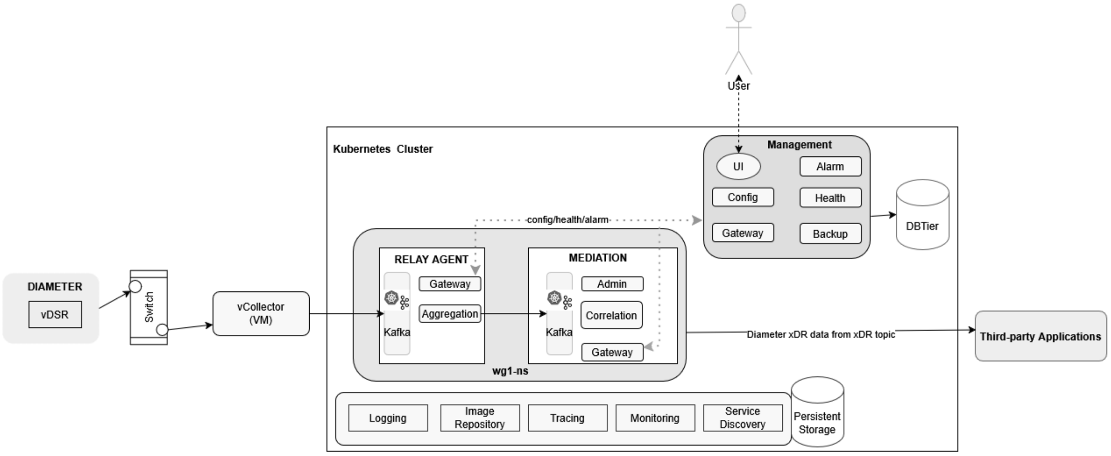
To facilitate high-volume data processing with a highly scalable solution, the Data Director architecture has been revamped and modularized into three distinct components.

The worker group has evolved into a logical entity that retains the same functionality as before, now encompassing both the DD Relay Agent and DD Mediation components.

- **Data Director Relay Agent:** The Data Director Relay Agent is engineered to handle high-volume data streams from Diameter nodes with a low data retention policy, while ensuring scalability and efficient data processing.
- **Data Director Mediation:** The Data Director Mediation is a vital component of the Data Director, leveraging high-data-retention Kafka clusters to integrate multiple data sources. It enables secure data delivery to third-party endpoints, supporting a range of data formats, including feeds, xDRs, trace, and KPIs.
- **Data Director Management:** The Data Director Management component provides a unified interface for managing and monitoring the Data Director. It offers a range of features, including a user-friendly UI, configuration management, alarm and health

monitoring, and backup and restore capabilities. Additionally, it supports the monitoring of Key Performance Indicators (KPIs), ensuring seamless data management and optimization.

Figure 2-2   OCNADD Centralized Deployment Architecture



3

OCNADD Features and Feature Specific Limits

This chapter details all major OCNADD features, features specific limits, and their functional behaviors.

3.1 Feature Specific Limits

This section defines capacity boundaries and limitations associated with the features.

The current release does not support Diameter configuration and visualization through the UI.

Table 3-1 OCNADD Feature Specific Limits

Description	Limit Value
Maximum number of worker groups supported in a Centralized Site	1
Maximum number of Kafka feeds for Diameter xDR per worker group: Maximum three Correlation feeds including all ACL feeds	2
Maximum number of vCollector configurations per worker group. **Note**: Each worker group will have a separate vCollector deployment	1

> **Note**
>
> The limits are controlled through Helm parameters. For more information, refer to the section "Global Parameters" of the *Oracle Communications Network Analytics Data Director Installation, Upgrade, and Fault Recovery Guide*.

3.2 Features List

This section details OCNADD features and their functional behaviors.

3.2.1 Data Governance

OCNADD provides data governance by managing the availability and usability of data in enterprise systems. It also ensures that the integrity and security of the data are maintained by adhering to all Oracle-defined data standards and policies for data usage rules.

3.2.2 High Availability

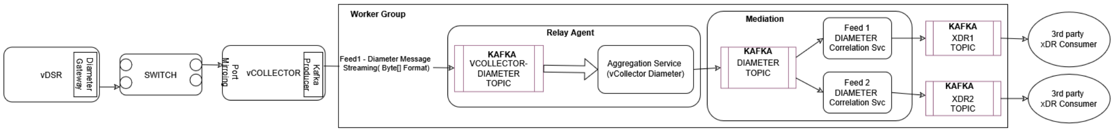
OCNADD supports a microservice-based architecture, and OCNADD instances are deployed in Cloud Native Environments (CNEs), which ensure high availability of services and auto-scaling based on resource utilization. In the case of pod failures, new service instances are spawned immediately.

In the event of a Kubernetes (K8s) cluster failure, the OCNADD deployment is restored to a different cluster using fault recovery mechanisms. For more information about fault recovery procedures, see the *Oracle Communications Network Analytics Data Director Installation, Upgrade, and Fault Recovery Guide*.

3.2.3 Data Filtering

OCNADD performs data filtering of Diameter messages on vCollector and sends only the filtered messages to the DD Relay Agent.

Figure 3-1 Diameter xDR Replication



Data filtering is managed only on vCollector in the current release for Diameter. Refer to the vCollector section in the OCNADD Features section.

> **Note**
>
> In the case of an upgrade, rollback, service restart, or if a configuration is created with the same name, duplicate messages will be sent by the aggregation and correlation service to avoid data loss.

3.2.4 vCollector

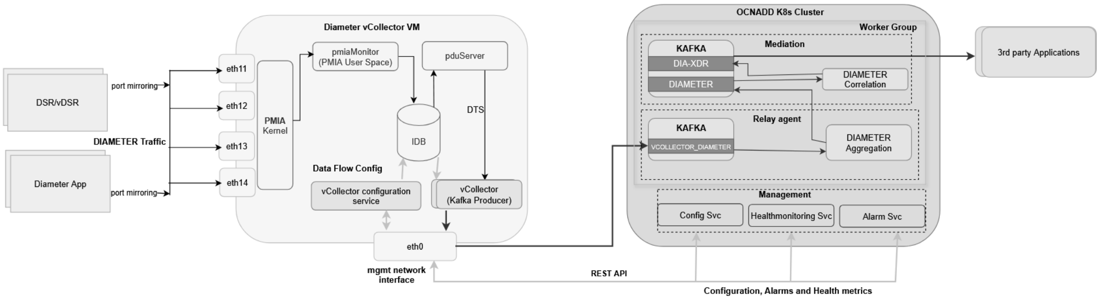
The vCollector provides a mechanism to acquire Diameter traffic from various network nodes, such as the Diameter Signaling Router (DSR) or any other Diameter application. Packet capturing is enabled via port mirroring to the virtual machine running Oracle proprietary software. The virtual machine solution is known as Diameter vCollector. This functionality includes:

1. Software that provides packet capture and filtering capabilities.
2. A Kafka-based producer client interface that transfers the captured packets to the Oracle packet broker solution over Kafka.
3. A configuration REST API to configure the traffic flow on the vCollector.
4. An in-memory database to store the configuration and serve as an intermediary buffer for the captured packets.

The Diameter vCollector reuses the OCPIC Probed Message Feeder (PMF) for packet capture and filtering capabilities. The following deployment modes for the vCollector are possible:

- It can support up to four capturing interfaces.
- The PMF software can be installed inside a virtual machine on the OpenStack cloud, with a virtual interface created on the virtual machine for capturing traffic. The vDSR and vCollector can run inside the same OpenStack cloud, and the port mirroring feature of the OpenStack cloud can be used to copy Diameter traffic from vDSR to vCollector.

Figure 3-2 vCollector Architecture



3.2.4.1 vCollector Integration with Data Director

This section describes the steps to integrate vCollector with Data Director to acquire Diameter traffic from vDSR using port mirroring. It requires that vCollector be installed and its initial topology configured.

See *Installing vCollector* chapter from the *Oracle Communications Network Analytics Data Director vCollector Installation Guide*.

After installing and initially configuring vCollector, continue with the creation of a Diameter feed using the section "vCollector Configuration" from the *Oracle Communications Network Analytics Data Director vCollector Installation Guide*.

3.2.4.2 vCollector Configuration

Note

- Only one configuration is supported in the current release.
- The name of the traffic flow in the configuration should not be in block letters and should not contain any special characters except "-".
- When the management gateway service lacks load balancer enablement, the APIRoot defaults to the service name; conversely, if load balancing is enabled, the APIRoot will be the LoadBalancer IP associated with the gateway service.

A. Create Configuration

Rest End Point: *<apiRoot>/ocnadd-configuration/{version}/configure/vcollector*

```
curl -k --location --cert-type P12 --cert /var/securityfiles/keystore/
serverKeyStore.p12:$OCNADD_SERVER_KS_PASSWORD --request PUT 'https://
ocnaddmanagementgateway:12889/ocnadd-configuration/v1/configure/vcollector' \
--header 'Content-Type: application/json' \
--data-raw '{
    "trafficFlowName": "<traffic-flow-name>",
    "vCollectorName": "<vcollector-config-name>",
    "userName": "<dd-ui-user-name>",
    "workerGroup": "<worker-group-name>",
    "relayAgentMediationGroup": {

"<siteName>:<workerGroupName>:<relayAgentNamespace>:<relayAgentClusterName>":
[

"<siteName>:<workerGroupName>:<mediationNamespace>:<mediationClusterName>"
        ]
        },
    "relayAgent": "agent-1",
    "tcInfo": {
        "tcName": "<traffic-flow-name>",
        "interfaces": [
            "vCollector_traffic_interface1",
            "vCollector_traffic_interface2"
        ],
        "filter": "<Diameter_Filter_Condition>",
        "enableDupIpPktSuppression": true,
        "enableSctpDechunking": false,
        "enableTcpFlowMng": false
    },
    "dfInfo": {
        "dfName": "<traffic-flow-name>",
        "wayMgmntAddr": [
            "<way_managemnt_IP1>",
            "<way_managemnt_IP2>"
        ]
    },
    "kafkaClusters": {
        "siteName": "SiteA",
        "primary": {
            "bootstrapServer": [
                "dd_kafka-bootstrap-IP1:9094",
                "dd_kafka-bootstrap-IP2:9094"
            ],
            "status": "Active",
            "topicName": "<vcollector-topic-name'>",
            "availableCapacity": 1234.56,
            "producerConfig": {
                "securityProtocol": "PLAINTEXT",
                "sslEnabledProtocol": "TLSv1.3",
                "ack": "0",
                "compression": "none",
                "maxRequestSize": 1048576,
                "batchSize": 500,
                "lingerMs": 100,
                "bufferMemory": 33554432,
                "retries": 3,
                "retryBackoffMs": 100,
                "requestTimeoutMs": 5000
            }
        },
        "secondary": null,
        "tertiary": null
    }
}'
```

Example:

```
curl -k --location --cert-type P12 --cert /var/securityfiles/keystore/
serverKeyStore.p12:$OCNADD_SERVER_KS_PASSWORD --request POST 'https://
ocnaddmanagementgateway:12889/ocnadd-configuration/v1/configure/vcollector' \
--header 'Content-Type: application/json' \
--data-raw '{
    "trafficFlowName": "diameter-flow",
    "userName": "admin",
    "workerGroup": "wg-1",
    "vCollectorName": "vcollector-config",
    "relayAgentMediationGroup": {
        "BLR:wg1:dd-relay:cluster.local": [
            "BLR:wg1:dd-med:cluster.local"
        ]
        },
    "relayAgent": "agent-1",
    "tcInfo": {
        "tcName": "diameter-flow",
        "interfaces": [
            "pmf-vc-01a_eth11",
            "pmf-vc-01a_eth12"
        ],
        "filter": "(src host 10.233.108.0 or src host 10.192.130.2 or src
host 10.192.130.3 or src host 10.192.130.4 or src host 10.192.130.5 or src
host 10.192.130.6 or src host 10.192.130.7 or src host 10.192.130.8)",
        "enableDupIpPktSuppression": false,
        "enableSctpDechunking": false,
        "enableTcpFlowMng": false
    },
    "dfInfo": {
        "dfName": "diameter-flow",
        "wayMgmntAddr": null
    },
    "kafkaClusters": {
        "siteName": "SiteA",
        "primary": {
            "bootstrapServer": [
                "10.10.10.11:9094",
                "10.10.10.12:9094"
            ],
            "status": "Active",
            "topicName": "vcollector",
            "availableCapacity": 1234.56,
            "producerConfig": {
                "securityProtocol": "PLAINTEXT",
                "sslEnabledProtocol": "TLSv1.3",
                "ack": "0",
                "compression": "none",
                "maxRequestSize": 1048576,
                "batchSize": 500,
                "lingerMs": 100,
                "bufferMemory": 33554432,
                "retries": 3,
                "retryBackoffMs": 100,
                "requestTimeoutMs": 5000
            }
        },
        "secondary": null,
        "tertiary": null
    }
}'
```

B. Update Configuration

Rest End Point: *<apiRoot>/ocnadd-configuration/{version}/configure/vcollector/{traffic-flow-name}*

```
curl -k --location --cert-type P12 --cert /var/securityfiles/keystore/
serverKeyStore.p12:$OCNADD_SERVER_KS_PASSWORD --request PUT 'https://
ocnaddmanagementgateway:12889/ocnadd-configuration/v1/configure/vcollector/
<traffic-flow-name>' \
--header 'Content-Type: application/json' \
--data-raw '{
    "trafficFlowName": "<traffic-flow-name>",
    "vCollectorName": "<vcollector-config-name>",
    "userName": "<dd-ui-user-name>",
    "workerGroup": "<worker-group-name>",
    "relayAgentMediationGroup": {

"<siteName>:<workerGroupName>:<relayAgentNamespace>:<relayAgentClusterName>":
[

"<siteName>:<workerGroupName>:<mediationNamespace>:<mediationClusterName>"
        ]
        },
    "relayAgent": "agent-1",
    "tcInfo": {
        "tcName": "<traffic-flow-name>",
        "interfaces": [
            "vCollector_traffic_interface1",
            "vCollector_traffic_interface2"
        ],
        "filter": "<Diameter_Filter_Condition>",
        "enableDupIpPktSuppression": true,
        "enableSctpDechunking": false,
        "enableTcpFlowMng": false
    },
    "dfInfo": {
        "dfName": "<traffic-flow-name>",
        "wayMgmntAddr": [
            "<way_managemnt_IP1>",
            "<way_managemnt_IP2>"
        ]
    },
    "kafkaClusters": {
        "siteName": "SiteA",
        "primary": {
            "bootstrapServer": [
                "dd_kafka-bootstrap-IP1:9094",
                "dd_kafka-bootstrap-IP2:9094"
            ],
            "status": "Active",
            "topicName": "<vcollector-topic-name'>",
            "availableCapacity": 1234.56,
            "producerConfig": {
                "securityProtocol": "PLAINTEXT",
                "sslEnabledProtocol": "TLSv1.3",
                "ack": "0",
                "compression": "none",
                "maxRequestSize": 1048576,
                "batchSize": 500,
                "lingerMs": 100,
                "bufferMemory": 33554432,
                "retries": 3,
                "retryBackoffMs": 100,
                "requestTimeoutMs": 5000
            }
        },
        "secondary": null,
        "tertiary": null
    }
}'
```

Example:

```
curl -k --location --cert-type P12 --cert /var/securityfiles/keystore/
serverKeyStore.p12:$OCNADD_SERVER_KS_PASSWORD --request PUT 'https://
ocnaddmanagementgateway:12889/ocnadd-configuration/v1/configure/vcollector/
diameter-flow' \
--header 'Content-Type: application/json' \
--data-raw '{
    "trafficFlowName": "diameter-flow",
    "userName": "admin",
    "workerGroup": "wg-1",
    "vCollectorName": "vcollector-config",
    "relayAgentMediationGroup": {
        "BLR:wg1:dd-relay:cluster.local": [
            "BLR:wg1:dd-med:cluster.local"
        ]
        },
    "relayAgent": "agent-1",
    "tcInfo": {
        "tcName": "diameter-flow",
        "interfaces": [
            "pmf-vc-01a_eth11",
            "pmf-vc-01a_eth12"
        ],
        "filter": "(src host 10.233.108.0 or src host 10.192.130.2 or src
host 10.192.130.3 or src host 10.192.130.4 or src host 10.192.130.5 or src
host 10.192.130.6 or src host 10.192.130.7 or src host 10.192.130.8)",
        "enableDupIpPktSuppression": false,
        "enableSctpDechunking": false,
        "enableTcpFlowMng": false
    },
    "dfInfo": {
        "dfName": "diameter-flow",
        "wayMgmntAddr": null
    },
    "kafkaClusters": {
        "siteName": "SiteA",
        "primary": {
            "bootstrapServer": [
                "10.10.10.11:9094",
                "10.10.10.12:9094"
            ],
            "status": "Active",
            "topicName": "vcollector",
            "availableCapacity": 1234.56,
            "producerConfig": {
                "securityProtocol": "PLAINTEXT",
                "sslEnabledProtocol": "TLSv1.3",
                "ack": "0",
                "compression": "none",
                "maxRequestSize": 1048576,
                "batchSize": 500,
                "lingerMs": 100,
                "bufferMemory": 33554432,
                "retries": 3,
                "retryBackoffMs": 100,
                "requestTimeoutMs": 5000
            }
        },
        "secondary": null,
        "tertiary": null
    }
}'
```

C. Delete Configuration

Rest End Point: *<apiRoot>/ocnadd-configuration/{version}/configure/vcollector/{trafficflowName}*

```
curl -k --location --cert-type P12 --cert /var/securityfiles/keystore/
serverKeyStore.p12:$OCNADD_SERVER_KS_PASSWORD --request DELETE 'https://
ocnaddmanagementgateway:12889/ocnadd-configuration/v1/configure/vcollector/
<traffic-flow-name>'
```

Example:

```
curl -k --location --cert-type P12 --cert /var/securityfiles/keystore/
serverKeyStore.p12:$OCNADD_SERVER_KS_PASSWORD --request DELETE 'https://
ocnaddmanagementgateway:12889/ocnadd-configuration/v1/configure/vcollector/
diameter-flow'
```

D. Get vCollector Configuration

Rest End Point:*{ apiRoot}/ocnadd-configuration/{version}/configuration/vcollector*

```
curl -k --location --cert-type P12 --cert /var/securityfiles/keystore/
serverKeyStore.p12:$OCNADD_SERVER_KS_PASSWORD --request GET 'https://
ocnaddmanagementgateway:12889/ocnadd-configuration/v1/configuration/
vcollector'
```

3.2.4.3 vCollector Filter

> **Note**
>
> In the current release, Diameter message filtering is supported only on vCollector with vCollector feed configuration.

The following is the format for adding a filter in vCollector:

```
((((((dcppi 47 or dcppi 46) or (dcppi 0 and (port 3868 or port 3871))) and
sctp(dia_appid 16777251)))
or
((tcp and (port 3868 or port 3871)) and tcp(dia_appid 16777251)))
or
(((((dcppi 47 or dcppi 46) or (dcppi 0 and (port 3868 or port 3871))) and
sctp(dia_appid 16777238)))
or
((tcp and (port 3868 or port 3871)) and tcp(dia_appid 16777238))))
```

The filter is a logical OR operation between two main conditions:

1. `((((dcppi 47 or dcppi 46) or (dcppi 0 and (port 3868 or port 3871))) and sctp(dia_appid 16777251))) or ((tcp and (port 3868 or port 3871)) and tcp(dia_appid 16777251))`
2. `((((dcppi 47 or dcppi 46) or (dcppi 0 and (port 3868 or port 3871))) and sctp(dia_appid 16777238))) or ((tcp and (port 3868 or port 3871)) and tcp(dia_appid 16777238))`

Condition 1 and 2: Both conditions have a similar structure, with the only difference being the `dia_appid value (16777251 vs 16777238)..`

Breaking down Condition 1 (similarly for Condition 2)

1. `(((dcppi 47 or dcppi 46) or (dcppi 0 and (port 3868 or port 3871))) and sctp(dia_appid 16777251))`
   - This part captures Diameter messages over SCTP (Stream Control Transmission Protocol) with `dia_appid` 16777251.
   - The conditions are:
     - `dcppi 47 or dcppi 46`: Capture packets with DCPPI (Diameter Credit-Control Protocol Identifier) values 47 or 46.

- `dcppi 0 and (port 3868 or port 3871)`: Capture packets with DCPPI value 0 and destination port 3868 or 3871 (common ports for Diameter).
- `sctp(dia_appid 16777251)`: Ensure the packet is SCTP and has a Diameter Application ID of 16777251.

2. `((tcp and (port 3868 or port 3871)) and tcp(dia_appid 16777251))`
   - This part captures Diameter messages over TCP (Transmission Control Protocol) with `dia_appid` 16777251.
   - The conditions are:
     - `tcp`: Ensure the packet is TCP.
     - `port 3868 or port 3871`: Capture packets with destination port 3868 or 3871.
     - `tcp(dia_appid 16777251)`: Ensure the Diameter Application ID is 16777251.

In Summary: The filter captures Diameter messages with specific Application IDs (16777251 and 16777238) over both SCTP and TCP, targeting ports 3868 and 3871, and considering different DCPPI values. The filter is designed to be flexible and capture a range of Diameter messages based on the specified conditions.

Diameter Application IDs:

- 16777251 is associated with the 3GPP (3rd Generation Partnership Project) Rx interface.
- 16777238 is associated with the 3GPP Gx interface.

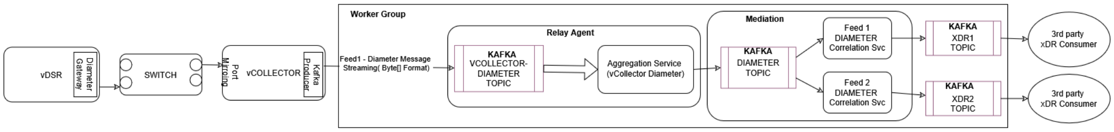
This filter is targeting Diameter traffic related to these interfaces, possibly for monitoring or analysis purposes in a telecommunications network.

3.2.5 Data Replication

OCNADD allows data replication functionality. The xDR data streams from OCNADD services can be replicated to multiple third-party applications simultaneously.

The following diagram depicts OCNADD data replication:

Figure 3-3 Diameter xDR Replication



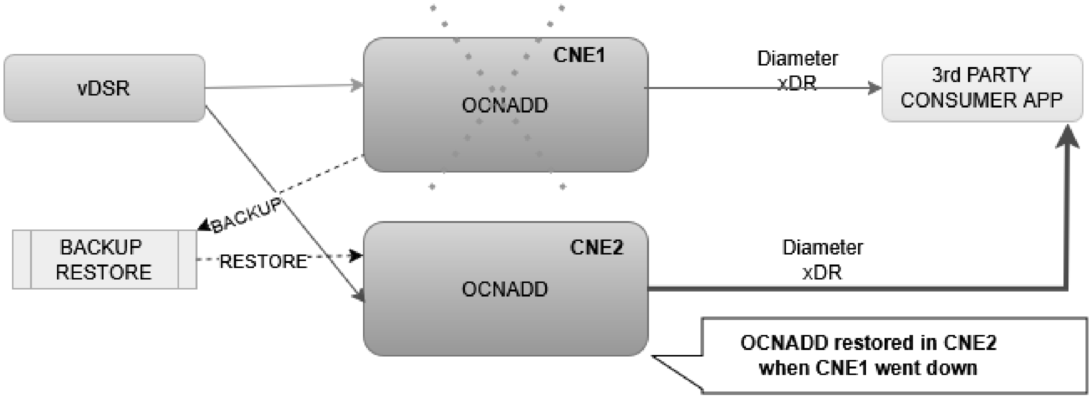
> **Note**
>
> The configuration of replication is not currently possible using the UI; the user can create another feed. Configuring multiple feeds may impact performance and increase latency.

3.2.6 Backup and Restore

OCNADD supports backup and restore to ensure high availability and quick recovery from failures such as cluster failure, database corruption, and so on. Two types of backup methods are supported: automated and manual backup. For more information on backup and restore, see the Oracle Communications Network Analytics Data Director Disaster Recovery Guide.

The following diagram depicts backup and restore supported by OCNADD:

Figure 3-4 Backup and Restore

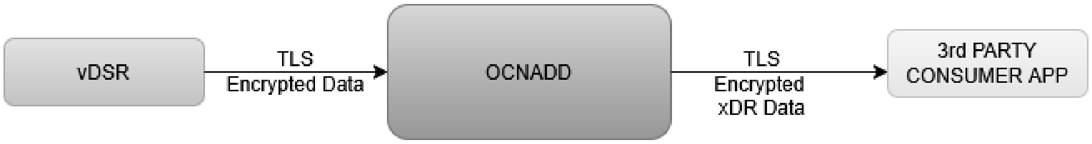


3.2.7 Secure Transport

OCNADD provides secure data communication between producer NFs and third-party consumer applications. All incoming and outgoing data streams from OCNADD are TLS encrypted.

The following diagram provides a secure transport by OCNADD:

Figure 3-5 Diameter Security

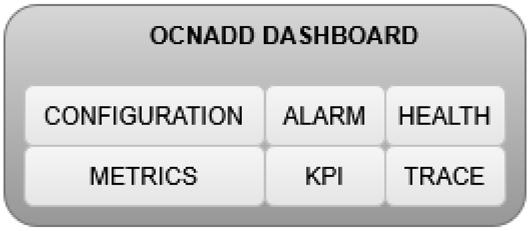


3.2.8 Operation Dashboard

OCNADD provides an operational dashboard that offers rich visualization of various metrics, KPIs, and alarms.

The dashboard can be depicted as follows:

Figure 3-6 Dashboard



3.2.9 Health Monitoring

OCNADD performs health monitoring to check the readiness and liveliness of each OCNADD service and raises alarms in case of service failure.

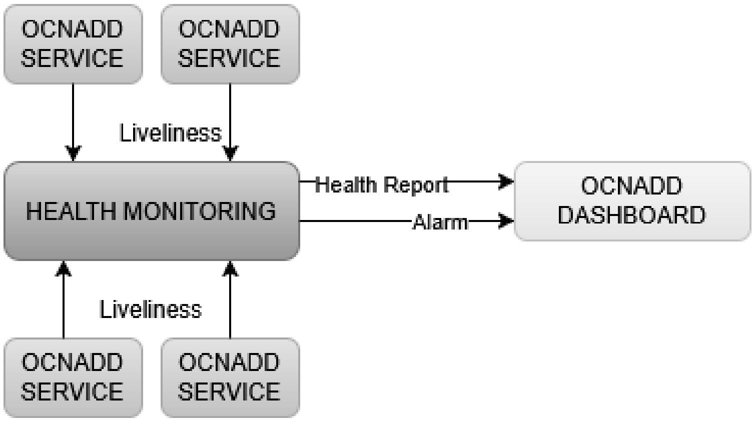
OCNADD conducts monitoring based on a heartbeat mechanism, where each OCNADD service instance registers with the Health Monitoring service and exchanges heartbeats with it. If a pod instance goes down, the Health Monitoring service raises an alarm. A few important scenarios when an alarm is raised are as follows:

- When the maximum number of replicas for a service has been instantiated
- When a service is in a down state
- When the CPU or memory threshold is reached

The health monitoring functionality allows OCNADD to generate a health report for each service on a periodic basis or on demand. These reports can be accessed using the OCNADD Dashboard. For more information about the dashboard, see Operation Dashboard.

The health monitoring service is depicted in the diagram below:

Figure 3-7 Health Monitoring

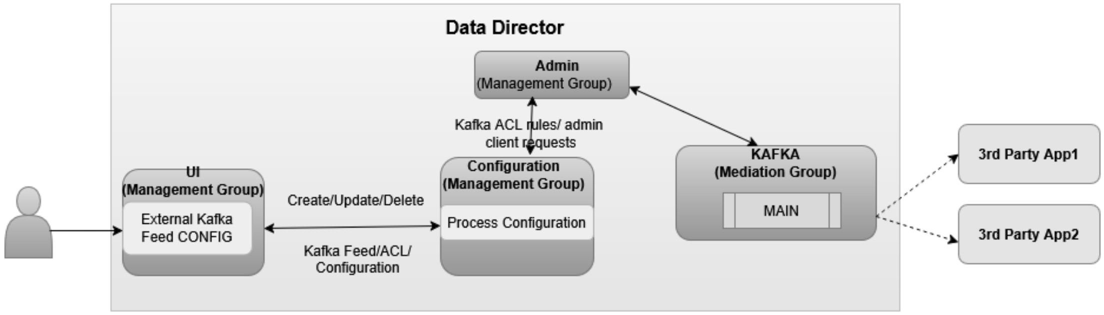


The health monitoring functionality also supports the collection of various metrics related to service resource utilization. It stores these metrics in the metric collection database tables. The health monitoring service generates alarms for missing heartbeats, connection breakdowns, and exceeding thresholds.

3.2.10 External Kafka Feeds

OCNADD supports external xDR Kafka consumer applications using external Kafka feeds. This enables third-party consumer applications to consume xDR directly from the Data Director Kafka xDR topic without the need for any egress adapter. OCNADD allows only those third-party applications that are authenticated and authorized by the Data Director Kafka service. The authorization of the applications is managed using the KAFKA ACL functionality. Access control for the external feed is defined at the time of Kafka feed creation, and currently, third-party applications are only allowed to consume (READ) from a particular topic using a specified consumer group.

Figure 3-8 External Kafka Feeds



The Data Director supports only the following for Diameter xDR external Kafka feeds:

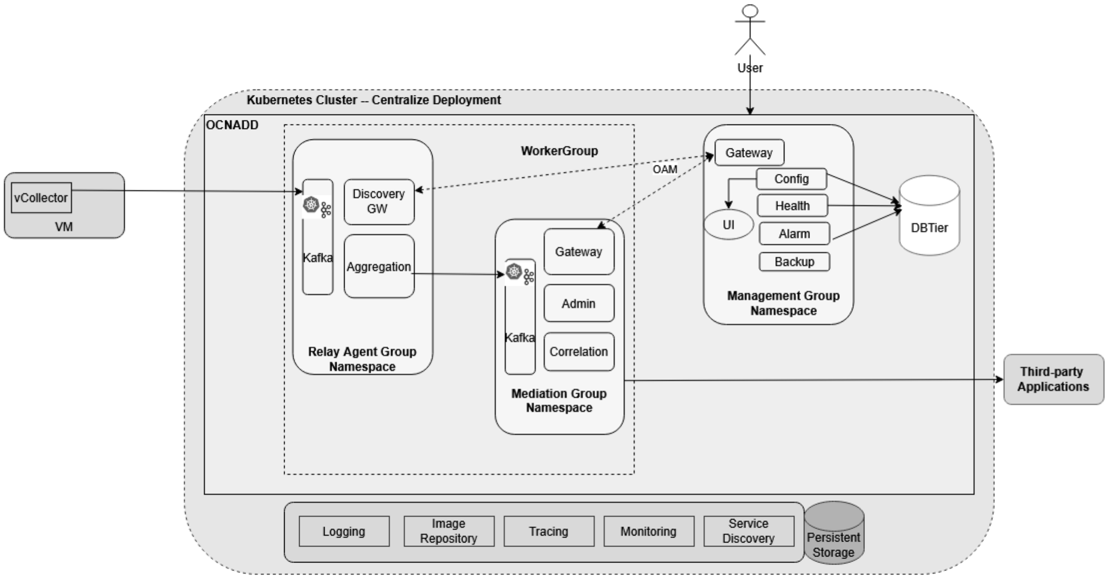
- Create, update, and delete the external Kafka feed using the UI.
- Authorization of the third-party Kafka consumer application for a particular user, consumer group, and optional hostname.
- Status reporting of the third-party Kafka consumer application using the external Kafka feed on the UI.
- Consumption rate reporting of the third-party Kafka consumer application using the external Kafka feed on the UI.

Authorization by Kafka requires clients to be authenticated by either SASL or SSL (mTLS). Therefore, external Kafka feed support requires certain settings to be enabled in the Kafka broker so that the Kafka service mandatorily authenticates Kafka clients. These properties are not enabled by default and must be configured in the Kafka service before any Kafka feed can work. See the "Enable Kafka Feed Configuration Support" section before creating any Kafka feed from the OCNADD UI.

3.2.11 Centralized Deployment

The OCNADD centralized deployment modes provide the separation of configuration and administration PODs from the traffic processing PODs. A single management POD group can serve multiple traffic processing POD groups (called Worker Groups), thereby saving resources for management PODs in very large customer deployments spanning multiple individual OCNADD sites. The **Management Group** of PODs maintains configuration and administration, health monitoring, alarms, and user interaction for all the individual worker groups.

Figure 3-9   Centralized Deployment



Management Group: A logical collection of the configuration and administration functions. It consists of Configuration, Alarm, Health Monitoring, Backup, and UI services.

Worker Group: A logical collection of traffic processing functions. The **Worker Group** represents the traffic processing functions and services, providing features like aggregation, filtering, correlation, and data feeds for third-party applications.

The worker group has evolved into a logical entity that retains the same functionality as before, now encompassing both the DD Relay Agent and DD Mediation components.

- **Data Director Relay Agent**: The Data Director Relay Agent is engineered to handle high-volume data streams from 5G Network Functions (NFs) with a low data retention policy, while ensuring scalability and efficient data processing.
  The Data Director Relay Agent is a composite component consisting of:
  - **Discovery Service Gateway:** Monitors the health of the Kafka cluster across multiple Data Director sites, facilitating communication between 5G Network Functions (NFs) and Data Director to retrieve and/or notify Kafka cluster information and its status.
  - **Kafka Cluster (low retention):** A Kafka cluster designed for high-throughput, providing low-latency, fault-tolerant, and scalable data processing. With a low retention period, it reduces dependency on underlying data storage to process and forward large amounts of data, ensuring high throughput by reducing performance degradations due to storage bottlenecks. This design enables the Kafka cluster to

  scale horizontally to accommodate increasing data volumes, making it ideal for handling high data ingestion rates typical of 5G networks.

  - **Aggregation Service:** Consumes traffic feed data produced by 5G Network Functions (NFs) from the Kafka cluster, providing a centralized processing point. It applies configurable ingress filtering to refine the data, sequences messages for proper ordering, and enriches the data with additional information. The processed data is then load-shared to different Data Director mediation instances for further processing, retention, and secured, reliable delivery to third-party consumers.

- **Data Director Mediation**: The Data Director Mediation is a vital component of the Data Director, leveraging high-data-retention Kafka clusters to integrate multiple data sources. It enables secure data delivery to third-party endpoints, supporting a range of data formats, including feeds, xDRs, trace, and KPIs.
  The Data Director Mediation is a composite component consisting of:
  - **Kafka Cluster:** Provides high-throughput, low-latency, fault-tolerant, and scalable data processing with higher retention.
  - **Correlation Service:** Enables the correlation of xDRs (eXtended Detail Records) for advanced data analysis.
  - **Gateway Service:** Facilitates secure communication with OAM (Operations, Administration, and Maintenance) systems.

Worker group names are formed using the worker group namespace and site or cluster name in the format "`worker_group_namespace:site_name`", where the site or cluster name is a global parameter in the Helm charts.

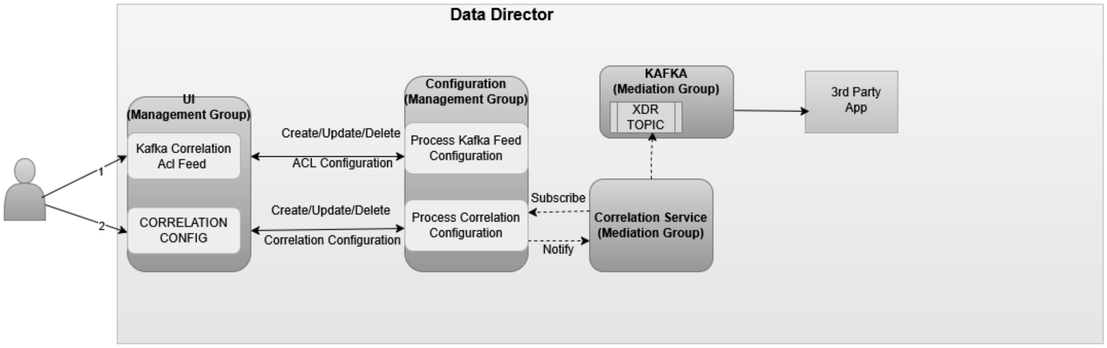
It is controlled by the `global.cluster.name` parameter.

Important points to consider for the Centralized deployment:

- In Centralized deployment mode, configuration management is decoupled from traffic processing, allowing traffic processing units to scale independently.
- Each worker group within a Centralized Data Director (DD) site can be configured with different capacities, but the maximum supported capacity for each worker group must be the same, encompassing both Relay Agent and Mediation components.
- There can be multiple worker groups in a centralized DD site, but in the current release, only one is recommended. Each worker group will support a traffic rate depending on the resource profiles of the worker group PODs. For example, if the worker group is dimensioned for processing 100K MPS traffic and the Centralized DD site needs to support 300–400K MPS, an additional worker group should be created on the centralized DD site.
- Metrics and alarms are generated separately for each worker group, including Relay Agent and Mediation components.
- The current release supports a fixed number of worker groups per Centralized DD site, limited to one.
- Fresh deployments in Centralized mode are supported with the new architecture.
- Upgrades from previous releases to Centralized deployment mode are recommended.
- The UI allows for the configuration of correlation configurations specific to each worker group. Refer to the UI guide for more information.

3.2.12 Diameter Correlation Feature

Figure 3-10 Diameter Correlation Feature



1. User needs to create kafka acl feed for correlation to consume xDRs from topic name provided in response.
2. User needs to create correlation configuration to start xDR generation

The Diameter correlation feature provides the capability to correlate messages of a network scenario that can be represented by a transaction, call, or session and generate a summary record. This summary record is known as an xDR. The generated summary records can provide deep insights and visibility into the customer network and can be useful in features such as:

- Network troubleshooting
- Revenue assurance
- Billing and CDR reconciliation
- Network performance KPIs and metrics
- Advanced analytics & observability

Network troubleshooting is one of the key features of the monitoring solution. The correlation capability helps the Data Director provide applications and utilities to perform troubleshooting of failing network scenarios, trace network scenarios across multiple Diameter nodes, and generate KPIs to provide network utilization and load. This feature enables network visibility and observability, as the KPIs and threshold alerts generated from the xDRs can be used to provide intuitive insights such as network efficiency reports in the form of network dashboards.

The xDRs generated by the Data Director can facilitate advanced descriptive and predictive network analytics. The correlation output in the form of xDRs can be fed into network analytics frameworks such as DAF to provide AI/ML capabilities that can be helpful in fraud detection and in predicting and preventing network spoofing and DOS attacks.

> **Note**
>
> In case of an upgrade, rollback, service restart, or if a configuration is created with the same name, duplicate messages/xDRs will be sent by the correlation service to avoid data loss.

3.2.12.1 Kafka Feed Configuration for Correlation

This section provides the details of the Kafka Feed configuration for correlation.

Prerequisites

It is mandatory to enable intra TLS for Kafka and create Kafka feed configuration with CORRELATED Feed Type to consume xDR (Extended Detailed Record) from OCNADD using Correlation Configurations.

3.2.12.1.1 Create ACL USER

Create ACL user prior to creating Kafka feeds. See Enable Kafka Feed Configuration Support.

3.2.12.1.2 Create Kafka Feed Configuration

To create Kafka Feed configuration, see Enable Kafka Feed Configuration Support.

3.2.12.1.3 Feed Type

- CORRELATED Feed Type:
  When the feed type is selected CORRELATED, aggregated data without a filter is used by the Correlation service to generate the xDRs.

  The source topic for correlation service would be the **DIAMETER** topic.

  The destination topic to consume data by third-party consumers is prefixed as **<kafka-feed-name>-CORRELATED topic**.

  > **Note**
  >
  > The user needs to trigger the corresponding Kafka ACL feed delete manually to delete the corresponding Topic, correlation config delete will not delete the topic.

- CORRELATED_FILTERED Feed Type
  CORRELATED_FILTERED Feed Type is not supported in the current release.

3.2.12.1.4 Diameter Feed Configuration

> **Note**
>
> CLI based configuration is supported for Diameter correlation configuration in the current release.

Configuration Parameters

Table 3-2 Configuration Parameters

Attribute Name	Data Type	P	Cardinality	Description
configurationName	String	M	1	The name of the configuration provided by the user for the correlation. This should be a unique name. It shall be mapped with Kafka ACL feed with **CORRELATED** type.
workerGroup	String	M	1	The name of the worker group in which the correlation configuration should be applied.
userName	String	M	1	The username provided by Dashboard GUI who is configuring the OCNADD correlation configuration.
dataStreamStartPoint	Enum	M	1	This parameter defines data stream points for correlation service from inbound topic. **Options:** EARLIEST: Start data stream from the beginning or resume from point of failure. LATEST: Proceed data stream from the current offset. **Default:** LATEST
inboundDataStreamName	String	M	1	Name of the source data stream from where the correlation service will start processing data. **Example:** DIAMETER: For aggregated data consumption with ACL feed type **CORRELATED**.

Table 3-2 (Cont.) Configuration Parameters

Attribute Name	Data Type	P	Cardinality	Description
outboundDataStreamName	String	M	1	Name of the destination data stream from where the correlation service will write an xDR, and a 3rd-party consumer app will start xDR streaming. **Example:** `<configurationName>-CORRELATED`: For aggregated xDR consumption with ACL feed type **CORRELATED**. ⓘ **Note** Filter (CORRELATED-FILTERED) is not supported

Table 3-2 (Cont.) Configuration Parameters

Attribute Name	Data Type	P	Cardinality	Description
				in the current release.
protocol	Enum	M	1	DIAMETER
xdrType	Enum	M	1	Type of xDR. **SUDR (SINGLE UNIT DETAILED RECORD)** – An xDR shall be generated for each message received in the correlation service. **TDR (TRANSACTION DETAILED RECORD)** – An xDR shall be generated for each transaction, including all messages of the transaction received in the correlation service. **Options:** • SUDR • TDR **Default:** SUDR

Table 3-2 (Cont.) Configuration Parameters

Attribute Name	Data Type	P	Cardinality	Description
supportedOptionalXdrContents	String[XdrContents]	M	1 to N	This configurable parameter provides an option to select xDR contents from the list of supported optional xDR contents. The xDR shall be generated with the selected xDR content, and the same will be sent to the 3rd-party app/ written into the outbound Kafka topic. • The mandatory xDR content shall always be present in the xDR. • By default, all xDR content shall be included in the xDR when present in the message. • If selected xDR contents are not present in the message, they will not be included in the xDR.
correlationMode	Enum	C	1	This provides an option to select the mode of transaction correlation for xDRs. The following definitions outline the correlation keys that will be maintained separately for each protocol type: **Protocol Type: DIAMETER** **Default mode:** SESSION_ID + ENDTOEND_ID + COMMAND_CODE **Options:** • SESSION_ID + ENDTOEND_ID + COMMAND_CODE • HOPBYHOP_ID + ENDTOEND_ID + COMMAND_CODE • IP + PORT + HOPBYHOP_ID + ENDTOEND_ID + COMMAND_CODE
maxTransactionWaitTime	Int	C	1	Maximum duration to wait for a response message for a transaction in milliseconds. **Range:** [2000–60000] **Default:** 30000

Table 3-2 (Cont.) Configuration Parameters

Attribute Name	Data Type	P	Cardinality	Description
includeMessageWithxDR	Enum	M	1	This property provides an option for the user to select whether a message will be included with the xDR or not, and if included, which part of the message. **Default:** NONE **Protocol Type: DIAMETER** • NONE: Only xDR shall be sent. • DIAMETER_JSON: xDR with JSON Diameter message.
supportedKpis	String[KPIs]	O	1 to N	This provides an option to the user to select a list of available supported KPIs.
storeXdrInDB	Boolean	O	1	It shall be set to false by default. The extended storage feature is not supported for **Protocol Type: DIAMETER**.
retentionTimeInDb	Int	C	1	It will be used for xDR records retention in DB. The value is in minutes. It must be provided when **storeXdrInDB = True**. Not supported for **Protocol Type: DIAMETER**.

Note

Create, update, and delete of Diameter Correlated Feed configurations is not supported from the UI.

A. Create Configuration

Rest End Point: *{apiRoot}/ocnadd-configuration/{version}/correlation*

```
curl -k --location --cert-type P12 --cert /var/securityfiles/keystore/
serverKeyStore.p12:$OCNADD_SERVER_KS_PASSWORD --request POST 'https://
ocnaddmanagementgateway:12889/ocnadd-configuration/v2/correlation' \
--header 'Content-Type: application/json' \
--data-raw '{
    "configurationName": "<diameter-feed-name>",
    "correlationConfig": {
        "configurationName": "<diameter-feed-name>",
        "userName": "<dd-ui-user-name>",
        "workerGroup": "<worker-group-name>",
        "relayAgentMediationGroup": {
```

```
"<siteName>:<workerGroupName>:<relayAgentNamespace>:<relayAgentClusterName>":
[

"<siteName>:<workerGroupName>:<mediationNamespace>:<mediationClusterName>"
           ]
        },
        "dataStreamStartPoint": "LATEST",
        "inboundDataStreamName": "DIAMETER",
        "outboundDataStreamName": "<diameter-feed-name-in-block-letters>-
CORRELATED",
        "supportedOptionalXdrContents": [
            "srcIp",
            "dstIp",
            "srcPort",
            "dsPort",
            "applicationId",
            "commandCode",
            "endToEndId",
            "imsi",
            "msisdn",
            "resultCode",
            "originalHost",
            "originalRealm",
            "destinationHost",
            "destinationRealm",
            "sessionId",
            "routeRecord",
            "vendorId",
            "authApplicationId",
            "subscriberStatus",
            "ratType",
            "visitedPlmnId",
            "serviceSelection",
            "absoluteTime",
            "relativeTime",
            "priorityLevel",
            "userLocationInfo3gpp",
            "mcc",
            "mnc",
            "imei",
            "sgsnMccMnc",
            "ggsnMccMnc",
            "qosClassIdentifier",
            "qosPriority",
            "tac",
            "cellId",
            "latitutde",
            "longitude",
            "way",
            "cancellationType",
            "addrType",
            "requestFlag",
            "answerFlag",
            "accApplicationId",
            "reqHeaderFlag",
            "ansHeaderFlag",
            "equipmentStatus",
            "alertReason",
            "sgsnNumber",
            "terminalInfo",
            "featureList",
            "userId",
            "mIPHomeAgentAddrType",
            "mipHomeAgentHost",
            "mIPHomeAgentAddress",
            "mIPHomeAgentRealm",
            "networkAccessMode",
            "visitedNetworkId",
            "requestCause",
            "terminationCause",
            "reAuthRequestType",
            "eventTrigger",
            "sessionReleaseCause",
            "ipCanType",
            "pdnType",
            "userLocation",
            "userLocationMNC",
            "userLocationECI",
            "userLocationLAC",
            "userLocationCISAC",
            "userLocationTAC",
            "preEmptionCapability",
            "preEmptionVulnerability",
            "pdnAddressV4",
            "pdnAddressV6",
            "apn",
            "ruleSpaceDecision",
            "ruleSpaceSuggestion",
            "nodeType",
            "transactionId"
        ],
        "xdrType": "TDR",
        "correlationMode": "<correlation-mode>",
        "maxTransactionWaitTime": 2000,
        "includeMessageWithxDR": "NONE",
        "ddMetadataRequired": false,
        "storeXdrInDB": false,
        "supportedKpis": [
            "TOTAL_TRANSACTION",
            "TOTAL_FAILED_TRANSACTION_PER_APPLICATION_ID",
            "TOTAL_SUCCESSFUL_TRANSACTION",
            "TOTAL_FAILED_TRANSACTION_PER_RESULT_CODE"
        ],
        "sourceFeedCorrCriteria": [],
        "retentionTimeInDb": 60,
        "diameterResponseIncluded": true,
        "corrProtocol": "DIAMETER"
    },
    "readyToStreamData": true
}'
```

Example:

```
curl -k --location --cert-type P12 --cert /var/securityfiles/keystore/
serverKeyStore.p12:$OCNADD_SERVER_KS_PASSWORD --request POST 'https://
ocnaddmanagementgateway:12889/ocnadd-configuration/v2/correlation' \
--header 'Content-Type: application/json' \
--data-raw '{
    "configurationName": "diameter-feed",
    "correlationConfig": {
        "configurationName": "diameter-feed",
        "userName": "admin",
        "workerGroup": "ocnadd-test:site-1",
        "relayAgentMediationGroup": {
           "BLR:wg1:dd-relay:cluster.local": [
              "BLR:wg1:dd-med:cluster.local"
           ]
        },
        "dataStreamStartPoint": "LATEST",
        "inboundDataStreamName": "DIAMETER",
        "outboundDataStreamName": "DIAMETER-FEED-CORRELATED",
        "supportedOptionalXdrContents": [
            "srcIp",
            "dstIp",
            "srcPort",
            "dsPort",
            "applicationId",
            "commandCode",
            "endToEndId",
            "imsi",
            "msisdn",
            "resultCode",
            "originalHost",
            "originalRealm",
            "destinationHost",
            "destinationRealm",
            "sessionId",
            "routeRecord",
            "vendorId",
            "authApplicationId",
            "subscriberStatus",
            "ratType",
            "visitedPlmnId",
            "serviceSelection",
            "absoluteTime",
            "relativeTime",
            "priorityLevel",
            "userLocationInfo3gpp",
            "mcc",
            "mnc",
            "imei",
            "sgsnMccMnc",
            "ggsnMccMnc",
            "qosClassIdentifier",
            "qosPriority",
            "tac",
            "cellId",
            "latitutde",
            "longitude",
            "way",
            "cancellationType",
            "addrType",
            "requestFlag",
            "answerFlag",
            "accApplicationId",
            "reqHeaderFlag",
            "ansHeaderFlag",
            "equipmentStatus",
            "alertReason",
            "sgsnNumber",
            "terminalInfo",
            "featureList",
            "userId",
            "mIPHomeAgentAddrType",
            "mipHomeAgentHost",
            "mIPHomeAgentAddress",
            "mIPHomeAgentRealm",
            "networkAccessMode",
            "visitedNetworkId",
            "requestCause",
            "terminationCause",
            "reAuthRequestType",
            "eventTrigger",
            "sessionReleaseCause",
            "ipCanType",
            "pdnType",
            "userLocation",
            "userLocationMNC",
            "userLocationECI",
            "userLocationLAC",
            "userLocationCISAC",
            "userLocationTAC",
            "preEmptionCapability",
            "preEmptionVulnerability",
            "pdnAddressV4",
            "pdnAddressV6",
            "apn",
            "ruleSpaceDecision",
            "ruleSpaceSuggestion",
            "nodeType",
            "transactionId"
        ],
        "xdrType": "TDR",
        "correlationMode": "IP+PORT+HOPBYHOP_ID+ENDTOEND_ID+COMMAND_CODE",
        "maxTransactionWaitTime": 2000,
        "includeMessageWithxDR": "NONE",
        "ddMetadataRequired": false,
        "storeXdrInDB": false,
        "supportedKpis": [
            "TOTAL_TRANSACTION",
            "TOTAL_FAILED_TRANSACTION_PER_APPLICATION_ID",
            "TOTAL_SUCCESSFUL_TRANSACTION",
            "TOTAL_FAILED_TRANSACTION_PER_RESULT_CODE"
        ],
        "sourceFeedCorrCriteria": [],
        "retentionTimeInDb": 60,
        "diameterResponseIncluded": true,
        "corrProtocol": "DIAMETER"
    },
    "readyToStreamData": true
}'
```

B. Update Configuration

Rest End Point: *<apiRoot>/ocnadd-configuration/{version}/correlation/{config-name}*

```
curl -k --location --cert-type P12 --cert /var/securityfiles/keystore/
serverKeyStore.p12:$OCNADD_SERVER_KS_PASSWORD --request PUT 'https://
ocnaddmanagementgateway:12889/ocnadd-configuration/v2/correlation/<diameter-
feed-name>' \
--header 'Content-Type: application/json' \
--data-raw '{
    "configurationName": "<diameter-feed-name>",
    "correlationConfig": {
        "configurationName": "<diameter-feed-name>",
        "userName": "<dd-ui-user-name>",
        "workerGroup": "<worker-group-name>",
        "relayAgentMediationGroup": {

"<siteName>:<workerGroupName>:<relayAgentNamespace>:<relayAgentClusterName>":
[

"<siteName>:<workerGroupName>:<mediationNamespace>:<mediationClusterName>"
           ]
        },
        "dataStreamStartPoint": "LATEST",
        "inboundDataStreamName": "DIAMETER",
        "outboundDataStreamName": "<diameter-feed-name-in-block-letters>-
CORRELATED",
        "supportedOptionalXdrContents": [
            "srcIp",
            "dstIp",
            "srcPort",
            "dsPort",
            "applicationId",
            "commandCode",
            "endToEndId",
            "imsi",
            "msisdn",
            "resultCode",
            "originalHost",
            "originalRealm",
            "destinationHost",
            "destinationRealm",
            "sessionId",
            "routeRecord",
            "vendorId",
            "authApplicationId",
            "subscriberStatus",
            "ratType",
            "visitedPlmnId",
            "serviceSelection",
            "absoluteTime",
            "relativeTime",
            "priorityLevel",
            "userLocationInfo3gpp",
            "mcc",
            "mnc",
            "imei",
            "sgsnMccMnc",
            "ggsnMccMnc",
            "qosClassIdentifier",
            "qosPriority",
            "tac",
            "cellId",
            "latitutde",
            "longitude",
            "way",
            "cancellationType",
            "addrType",
            "requestFlag",
            "answerFlag",
            "accApplicationId",
            "reqHeaderFlag",
            "ansHeaderFlag",
            "equipmentStatus",
            "alertReason",
            "sgsnNumber",
            "terminalInfo",
            "featureList",
            "userId",
            "mIPHomeAgentAddrType",
            "mipHomeAgentHost",
            "mIPHomeAgentAddress",
            "mIPHomeAgentRealm",
            "networkAccessMode",
            "visitedNetworkId",
            "requestCause",
            "terminationCause",
            "reAuthRequestType",
            "eventTrigger",
            "sessionReleaseCause",
            "ipCanType",
            "pdnType",
            "userLocation",
            "userLocationMNC",
            "userLocationECI",
            "userLocationLAC",
            "userLocationCISAC",
            "userLocationTAC",
            "preEmptionCapability",
            "preEmptionVulnerability",
            "pdnAddressV4",
            "pdnAddressV6",
            "apn",
            "ruleSpaceDecision",
            "ruleSpaceSuggestion",
            "nodeType",
            "transactionId"
        ],
        "xdrType": "TDR",
        "correlationMode": "<correlation-mode>",
        "maxTransactionWaitTime": 2000,
        "includeMessageWithxDR": "NONE",
        "ddMetadataRequired": false,
        "storeXdrInDB": false,
        "supportedKpis": [
            "TOTAL_TRANSACTION",
            "TOTAL_FAILED_TRANSACTION_PER_APPLICATION_ID",
            "TOTAL_SUCCESSFUL_TRANSACTION",
            "TOTAL_FAILED_TRANSACTION_PER_RESULT_CODE"
        ],
        "sourceFeedCorrCriteria": [],
        "retentionTimeInDb": 60,
        "diameterResponseIncluded": true,
        "corrProtocol": "DIAMETER"
    },
    "readyToStreamData": true
}'
```

Example:

```
curl -k --location --cert-type P12 --cert /var/securityfiles/keystore/
serverKeyStore.p12:$OCNADD_SERVER_KS_PASSWORD --request PUT 'https://
ocnaddmanagementgateway:12889/ocnadd-configuration/v2/correlation/diameter-
feed' \
--header 'Content-Type: application/json' \
--data-raw '{
    "configurationName": "diameter-feed",
    "correlationConfig": {
        "configurationName": "diameter-feed",
        "userName": "admin",
        "workerGroup": "ocnadd-test:site-1",
        "relayAgentMediationGroup": {
            "BLR:wg1:dd-relay:cluster.local": [
              "BLR:wg1:dd-med:cluster.local"
           ]
        },
        "dataStreamStartPoint": "LATEST",
        "inboundDataStreamName": "DIAMETER",
        "outboundDataStreamName": "DIAMETER-FEED-CORRELATED",
        "supportedOptionalXdrContents": [
            "srcIp",
            "dstIp",
            "srcPort",
            "dsPort",
            "applicationId",
            "commandCode",
            "endToEndId",
            "imsi",
            "msisdn",
            "resultCode",
            "originalHost",
            "originalRealm",
            "destinationHost",
            "destinationRealm",
            "sessionId",
            "routeRecord",
            "vendorId",
            "authApplicationId",
            "subscriberStatus",
            "ratType",
            "visitedPlmnId",
            "serviceSelection",
            "absoluteTime",
            "relativeTime",
            "priorityLevel",
            "userLocationInfo3gpp",
            "mcc",
            "mnc",
            "imei",
            "sgsnMccMnc",
            "ggsnMccMnc",
            "qosClassIdentifier",
            "qosPriority",
            "tac",
            "cellId",
            "latitutde",
            "longitude",
            "way",
            "cancellationType",
            "addrType",
            "requestFlag",
            "answerFlag",
            "accApplicationId",
            "reqHeaderFlag",
            "ansHeaderFlag",
            "equipmentStatus",
            "alertReason",
            "sgsnNumber",
            "terminalInfo",
            "featureList",
            "userId",
            "mIPHomeAgentAddrType",
            "mipHomeAgentHost",
            "mIPHomeAgentAddress",
            "mIPHomeAgentRealm",
            "networkAccessMode",
            "visitedNetworkId",
            "requestCause",
            "terminationCause",
            "reAuthRequestType",
            "eventTrigger",
            "sessionReleaseCause",
            "ipCanType",
            "pdnType",
            "userLocation",
            "userLocationMNC",
            "userLocationECI",
            "userLocationLAC",
            "userLocationCISAC",
            "userLocationTAC",
            "preEmptionCapability",
            "preEmptionVulnerability",
            "pdnAddressV4",
            "pdnAddressV6",
            "apn",
            "ruleSpaceDecision",
            "ruleSpaceSuggestion",
            "nodeType",
            "transactionId"
        ],
        "xdrType": "TDR",
        "correlationMode": "IP+PORT+HOPBYHOP_ID+ENDTOEND_ID+COMMAND_CODE",
        "maxTransactionWaitTime": 2000,
        "includeMessageWithxDR": "NONE",
        "ddMetadataRequired": false,
        "storeXdrInDB": false,
        "supportedKpis": [
            "TOTAL_TRANSACTION",
            "TOTAL_FAILED_TRANSACTION_PER_APPLICATION_ID",
            "TOTAL_SUCCESSFUL_TRANSACTION",
            "TOTAL_FAILED_TRANSACTION_PER_RESULT_CODE"
        ],
        "sourceFeedCorrCriteria": [],
        "retentionTimeInDb": 60,
        "diameterResponseIncluded": true,
        "corrProtocol": "DIAMETER"
    },
    "readyToStreamData": true
}'
```

C. Delete Configuration

Rest End Point: *<apiRoot>/ocnadd-configuration/{version}/correlation/{configurationName}*

```
curl -k --location --cert-type P12 --cert /var/securityfiles/keystore/
serverKeyStore.p12:$OCNADD_SERVER_KS_PASSWORD --request DELETE 'https://
ocnaddmanagementgateway:12889/ocnadd-configuration/v2/correlation/<diameter-
feed-name>' \
```

Example:

```
curl -k --location --cert-type P12 --cert /var/securityfiles/keystore/
serverKeyStore.p12:$OCNADD_SERVER_KS_PASSWORD --request DELETE 'https://
ocnaddmanagementgateway:12889/ocnadd-configuration/v2/correlation/diameter-
feed' \
```

D. Get Diameter Correlation Configuration

Rest End Point: *{ apiRoot}/ocnadd-configuration/{version}/correlation/configurations*

```
curl -k --location --cert-type P12 --cert /var/securityfiles/keystore/
serverKeyStore.p12:$OCNADD_SERVER_KS_PASSWORD --request GET 'https://
ocnaddmanagementgateway:12889/ocnadd-configuration/v2/correlation/
configurations' \
```

E. Get Specific Diameter Correlation Configuration

Rest End Point: *{ apiRoot}/ocnadd-configuration/{version}/correlation/{config-name}*

```
curl -k --location --cert-type P12 --cert /var/securityfiles/keystore/
serverKeyStore.p12:$OCNADD_SERVER_KS_PASSWORD --request GET 'https://
ocnaddmanagementgateway:12889/ocnadd-configuration/v2/correlation/<diameter-
feed-name> \
```

Example:

```
curl -k --location --cert-type P12 --cert /var/securityfiles/keystore/
serverKeyStore.p12:$OCNADD_SERVER_KS_PASSWORD --request GET 'https://
ocnaddmanagementgateway:12889/ocnadd-configuration/v2/correlation/diameter-
feed' \
```

3.2.12.1.5 XDR Content

This section provides the details of the xDR mandatory and optional xRD content.

Mandatory xDR Content

Table 3-3 Mandatory xDR Content

Field	Data Type	Presence	Description
version	String	M	Version number of xDR content.
configurationName	String	M	Correlation configuration name. This can be used by a 3rd-party consumer to distinguish between multiple configuration xDRs when the same outbound Kafka topic is used.
beginTime	String(UTC time)	M	Date and time in milliseconds of the first message of the xDR. **Example**: "2023-01-23T07:03:36.311Z"
endTime	String(UTC time)	M	Date and time of the last event in the transaction (last message or timeout). **Example**: "2023-01-23T07:03:39.311Z"
xdrStatus	Enum	M	xDR status of the correlated transaction. **Value:** SUDR, COMPLETE, TIMER_EXPIRY, NOT_MATCHED

Optional xDR Content

> **Note**
>
> The mandatory fields will always be present in xDRs and optional fields will be present based on their availability in the message.

Table 3-4 Optional xDR Content

<table>
<tr><th>Field Name</th><th>Data Type</th><th>Presence</th><th>Description</th></tr>
<tr><td>totalPduCount</td><td>Integer</td><td>O</td><td>The total number of messages are present in transaction.
It must be selected in xDR when correlation mode is not set to SUDR.
• – An xDR is generate with request message and response message then total-pdu-count is set to 2 or total no. of message of transaction.
– An xDR is generate with either only request message or response message then total-pdu-count is set to 1.</td></tr>
<tr><td>totalLength</td><td>Integer</td><td>O</td><td>Total sum of messages is present in transaction and It will be in bytes format.
It will be updated when includeMessageWithxDR is not NONE.</td></tr>
<tr><td>transactionId</td><td>String</td><td>O</td><td>The unique identifier of transaction.
It must be selected in xDR when correlation mode is not set to SUDR.</td></tr>
<tr><td>transactionTime</td><td>String</td><td>O</td><td>Duration of the complete transaction(endTime-beginTime). In case of timeout the transaction time will be calculated between transactions begin time and timeout event.
It must be selected in xDR when correlation mode is not set to SUDR.
It will be in milisecond.
<b>Example</b>: 1000</td></tr>
<tr><td>way</td><td>String</td><td>O</td><td>The direction of the TCP connection relative to the observation point, as indicated by the source.
The data will be extracted from header 'Flags' and populated from the first occurrence of the relevant information in the message.
The mapped label value will be present in the xDRs.
<table><tr><th>Value</th><th>Mapped Label</th></tr><tr><td>0</td><td>Uplink</td></tr><tr><td>1</td><td>Downlink</td></tr></table></td></tr>
<tr><td>srcIp</td><td>String</td><td>O</td><td>The source IP address of the initial message in the session or transaction.
The data will be extracted from metadata-list and populated from the first occurrence of the relevant information in the message.</td></tr>
<tr><td>dstIp</td><td>String</td><td>O</td><td>The destination IP address of the initial message in the session or transaction.
The data will be extracted from metadata-list and populated from the first occurrence of the relevant information in the message.</td></tr>
<tr><td>srcPort</td><td>String</td><td>O</td><td>The TCP port used by the application on the originating IP address.
The data will be extracted from metadata-list and populated from the first occurrence of the relevant information in the message.</td></tr>
</table>

Table 3-4   (Cont.) Optional xDR Content

Field Name	Data Type	Presence	Description
dstPort	String	O	The TCP port used by the application on the destination IP address. The data will be extracted from metadata-list and populated from the first occurrence of the relevant information in the message.

Table 3-4 (Cont.) Optional xDR Content

<table>
<tr><th>Field Name</th><th>Data Type</th><th>Presence</th><th>Description</th></tr>
<tr><td>applicationId</td><td>String</td><td>O</td><td>The applicationId is used to identify which diameter Interface the message is applicable for.
The data will be extracted from header 'ApplicationId' and populated from the first occurrence of the relevant information in the message.
The mapped label value will be present in the xDRs.
<table>
<tr><th>Value</th><th>Mapped Label</th></tr>
<tr><td>0</td><td>Diameter Common Messages</td></tr>
<tr><td>1</td><td>Diameter NASREQ Application</td></tr>
<tr><td>2</td><td>Diameter Mobile IPv4 Application</td></tr>
<tr><td>3</td><td>Diameter Base Accounting</td></tr>
<tr><td>4</td><td>Diameter Credit-Control Application</td></tr>
<tr><td>5</td><td>Diameter EAP</td></tr>
<tr><td>6</td><td>Diameter Session Initiation Protocol (SIP) Application</td></tr>
<tr><td>16777216</td><td>3GPP Cx/Dx</td></tr>
<tr><td>16777217</td><td>3GPP Sh/Ph</td></tr>
<tr><td>16777218</td><td>3GPP Re/Rf</td></tr>
<tr><td>16777219</td><td>3GPP Wx</td></tr>
<tr><td>16777220</td><td>3GPP Zn</td></tr>
<tr><td>16777221</td><td>3GPP Zh</td></tr>
<tr><td>16777222</td><td>3GPP Gq</td></tr>
<tr><td>16777223</td><td>3GPP Gmb</td></tr>
<tr><td>16777224</td><td>3GPP Gx</td></tr>
<tr><td>16777225</td><td>3GPP Gx over Gy</td></tr>
<tr><td>16777226</td><td>3GPP MM10</td></tr>
<tr><td>16777229</td><td>3GPP Rx</td></tr>
<tr><td>16777230</td><td>3GPP Pr</td></tr>
<tr><td>16777231</td><td>ETSI e4</td></tr>
<tr><td>16777235</td><td>ITU-T Rs</td></tr>
<tr><td>16777236</td><td>3GPP Rx (Policy and Charging Control over Rx)</td></tr>
<tr><td>16777238</td><td>Gx</td></tr>
<tr><td>16777250</td><td>STa/SWa</td></tr>
<tr><td>16777251</td><td>S6a</td></tr>
<tr><td>16777252</td><td>S13</td></tr>
<tr><td>16777255</td><td>SLg</td></tr>
<tr><td>16777264</td><td>SWm</td></tr>
<tr><td>16777265</td><td>SWx</td></tr>
<tr><td>16777266</td><td>Gxx</td></tr>
<tr><td>16777267</td><td>S9</td></tr>
<tr><td>16777268</td><td>Zpn</td></tr>
<tr><td>16777272</td><td>S6b</td></tr>
<tr><td>16777291</td><td>SLh</td></tr>
<tr><td>16777292</td><td>SGmb</td></tr>
<tr><td>16777302</td><td>Sy</td></tr>
<tr><td>16777303</td><td>Sd</td></tr>
</table>
</td></tr>
</table>

Table 3-4 (Cont.) Optional xDR Content

<table>
<tr><th>Field Name</th><th>Data Type</th><th>Presence</th><th>Description</th></tr>
<tr><td></td><td></td><td></td><td><table>
<tr><td>16777308</td><td>S7a</td></tr>
<tr><td>16777309</td><td>Tsp</td></tr>
<tr><td>16777310</td><td>S6m</td></tr>
<tr><td>16777311</td><td>T4</td></tr>
<tr><td>16777312</td><td>S6c</td></tr>
<tr><td>16777313</td><td>SGd</td></tr>
<tr><td>16777318</td><td>S15</td></tr>
<tr><td>16777319</td><td>S9a</td></tr>
<tr><td>16777320</td><td>S9a*</td></tr>
</table></td></tr>
</table>

Table 3-4 (Cont.) Optional xDR Content

<table>
<tr><th>Field Name</th><th>Data Type</th><th>Presence</th><th>Description</th></tr>
<tr><td>commandCode</td><td>String</td><td>O</td><td>A Command Code is a unique identifier that is used to identify a specific Diameter command and It is used in order to communicate the command associated with the message.
It will be populated from the first occurrence of the relevant information in the message and populated from the first occurrence of the relevant information in the message.
The mapped label value will be present in the xDRs.
<table>
<tr><th>Value</th><th>Mapped Label</th></tr>
<tr><td>0</td><td>Diameter Common Messages</td></tr>
<tr><td>257</td><td>CER/CEA, Capabilities-Exchange-Request/-Answer</td></tr>
<tr><td>258</td><td>RAR/RAA, Re-Auth-Request/-Answer</td></tr>
<tr><td>260</td><td>AMR/AMA, AA-Mobile-Node-Request/-Answer</td></tr>
<tr><td>262</td><td>HAR/HAA, Home-Agent-MIP-Request/-Answer</td></tr>
<tr><td>265</td><td>AAR/AAA, AA-Request/-Answer</td></tr>
<tr><td>268</td><td>DER/DEA, Diameter-EAP-Request/-Answer</td></tr>
<tr><td>271</td><td>ACR/ACA, Accounting-Request/-Answer</td></tr>
<tr><td>272</td><td>CCR/CCA, Credit-Control-Request/-Answer</td></tr>
<tr><td>274</td><td>ASR/ASA, Abort-Session-Request/-Answer</td></tr>
<tr><td>275</td><td>STR/STA, Session-Termination-Request/-Answer</td></tr>
<tr><td>280</td><td>DWR/DWA, Device-Watchdog-Request/Answer</td></tr>
<tr><td>282</td><td>DPR/DPA, Disconnect-Peer-Request/Answer:DPR/DPA</td></tr>
<tr><td>300</td><td>UAR/UAA, User-Authorization-Request/-Answer</td></tr>
<tr><td>301</td><td>SAR/SAA, Server-Assignment-Request/-Answer</td></tr>
<tr><td>302</td><td>LIR/LIA, Location-Info-Request/-Answer</td></tr>
<tr><td>303</td><td>MAR/MAA, Multimedia-Auth-Request/-Answer</td></tr>
<tr><td>304</td><td>RTR/RTA, Registration-Termination-Request/-Answer</td></tr>
<tr><td>305</td><td>PPR/PPA, Push-Profile-Request/-Answer</td></tr>
<tr><td>306</td><td>UDR/UDA, User-Data-Request/-Answer</td></tr>
<tr><td>307</td><td>PUR/PUA, Profile-Update-Request/-Answer:PUR/PUA</td></tr>
<tr><td>308</td><td>SNR/SNA, Subscribe-Notifications-Request/-Answer</td></tr>
<tr><td>309</td><td>PNR/PNA, Push-Notification-Request/-Answer:PNR/PNA</td></tr>
</table>
</td></tr>
</table>

Table 3-4 (Cont.) Optional xDR Content

<table>
<tr><th>Field Name</th><th>Data Type</th><th>Presence</th><th>Description</th></tr>
<tr><td></td><td></td><td></td><td>
<table>
<tr><td>310</td><td>BIR/BIA, Boostrapping-Info-Request/ Answer</td></tr>
<tr><td>311</td><td>MPR/MPA, Message-Process-Request/Answer</td></tr>
<tr><td>316</td><td>ULR/ULA, Update-Location-Request/-Answer</td></tr>
<tr><td>317</td><td>CLR/CLA, Cancel-Location-Request/-Answer</td></tr>
<tr><td>318</td><td>AIR/AIA, Authentication-Information-Request/-Answer</td></tr>
<tr><td>319</td><td>IDR/IDA, Insert-Subscriber-Data-Request/-Answer</td></tr>
<tr><td>320</td><td>DSR/DSA, Delete-Subscriber-Data-Request/-Answer</td></tr>
<tr><td>321</td><td>PUER/PUA, Purge-UE-Request/-Answer</td></tr>
<tr><td>322</td><td>RSR/RSA, Reset-Request/-Answer</td></tr>
<tr><td>323</td><td>NOR/NOA, Notify-Request/-Answer</td></tr>
<tr><td>324</td><td>ECR/ECA, ME-Identity-Check-Request/-Answe</td></tr>
<tr><td>500</td><td>RAR/RAA, Registration-Authorization-Request/-Answer</td></tr>
<tr><td>501</td><td>LUR/LUA, Location-Update-Request/-Answer</td></tr>
<tr><td>504</td><td>SIR/SIA, Security-Information-Request/-Answer</td></tr>
<tr><td>505</td><td>SIR/SIA, Security-Information-Request/-Answer</td></tr>
<tr><td>8388620</td><td>PLR/PLA, Provide-Location-Request/-Answer</td></tr>
<tr><td>8388621</td><td>LLR/LLA, Location-Report-Request/-Answer</td></tr>
<tr><td>8388622</td><td>RIR/RIA, LCS-Routing-Info-Request/-Answer</td></tr>
<tr><td>8388635</td><td>SLR/SLA, Spending-Limit-Request/-Answer</td></tr>
<tr><td>8388636</td><td>SNR/SNA, Spending-Status-Notification-Request/-Answer</td></tr>
<tr><td>8388637</td><td>TSR/TSA, TDF-Session-Request/-Answer</td></tr>
<tr><td>8388638</td><td>UVR/UVA, Update-VCSG-Location-Request/-Answer</td></tr>
<tr><td>8388639</td><td>DAR/DAA, Device-Action-Request/-Answer</td></tr>
<tr><td>8388640</td><td>DNR/DNA, Device-Notification-Request/-Answer</td></tr>
<tr><td>8388641</td><td>SIR/SIA, Subscriber-Information-Request/-Answer</td></tr>
<tr><td>8388642</td><td>CVR/CVA, Cancel-VCSG-Location-Request/-Answer</td></tr>
<tr><td>8388643</td><td>DTR/DTA, Device-Trigger-Request-/ Answer</td></tr>
</table>
</td></tr>
</table>

Table 3-4 (Cont.) Optional xDR Content

<table>
<tr><th>Field Name</th><th>Data Type</th><th>Presence</th><th>Description</th></tr>
<tr><td></td><td></td><td></td><td>
<table>
<tr><td>8388644</td><td>DRR/DRA, Delivery-Report-Request-/ Answer</td></tr>
<tr><td>8388645</td><td>OFR/OFA, MO-Forward-Short-MessageRequest/-Answer</td></tr>
<tr><td>8388646</td><td>TFR/TFA, MT-Forward-Short-MessageRequest/-Answer</td></tr>
<tr><td>8388647</td><td>SRR/SRA, Send-Routing-Info-for-SMRequest/-Answer</td></tr>
<tr><td>8388648</td><td>ALR/ALA, Alert-Service-Centre-Request/-Answer</td></tr>
<tr><td>8388649</td><td>RDR/RDA, Report-SM-Delivery-Status-Request/-Answer</td></tr>
<tr><td>8388656</td><td>TER/TEA, Trigger-Establishment-Request/-Answer</td></tr>
<tr><td>8388662</td><td>GAR/GAA, GCS-Action-Request/ Answer</td></tr>
<tr><td>8388663</td><td>GNR/GNA, GCS-Notification-Request/ Answer</td></tr>
<tr><td>8388664</td><td>PIR/PIA, ProSe-Subscriber-Information-Request/Answer</td></tr>
<tr><td>8388665</td><td>UPR/UPA, Update-ProSe-Subscriber-Data-Request/Answer</td></tr>
<tr><td>8388666</td><td>PNR/PNA, ProSe-Notify-Request/ Answer</td></tr>
<tr><td>8388668</td><td>PAR/PAA, ProSe-Authorization-Request/Answer</td></tr>
<tr><td>8388669</td><td>PDR/PDA, ProSe-Discovery-Request/ Answer</td></tr>
<tr><td>8388670</td><td>PMR/PMA, ProSe-Match-Request/ Answer</td></tr>
<tr><td>8388671</td><td>PIR/PIA, ProSe-Match-Report-Info-Request/Answer</td></tr>
<tr><td>8388672</td><td>PRR/PRA, ProSe-Proximity-Request/ Answer</td></tr>
<tr><td>8388673</td><td>PDR/PDA, ProSe-Location-Update-Request/Answer</td></tr>
<tr><td>8388674</td><td>ALR/ALA, ProSe-Alert-Request/ Answer</td></tr>
<tr><td>8388675</td><td>RPR/RPA, ProSe-Cancellation-Request/Answer</td></tr>
<tr><td>8388676</td><td>PXR/PXA, ProXimity-Action-Request/ Answer</td></tr>
<tr><td>8388713</td><td>PSR/PSA, ProSe-Initial-Location-Information-Request/Answer</td></tr>
<tr><td>8388718</td><td>CIR/CIA, Configuration-Information-Request/Answer</td></tr>
<tr><td>8388719</td><td>RIR/RIA, Reporting-Information-Request/Answer</td></tr>
<tr><td>8388720</td><td>NRR/NRA, Non-Aggregated-RUCI-Report-Request/Answer</td></tr>
<tr><td>8388721</td><td>ARR/ARA, Aggregated-RUCI-Report-Request/Answer</td></tr>
</table>
</td></tr>
</table>

Table 3-4 (Cont.) Optional xDR Content

<table>
<tr><th>Field Name</th><th>Data Type</th><th>Presence</th><th>Description</th></tr>
<tr><td></td><td></td><td></td><td>
<table>
<tr><td>8388722</td><td>MUR/MUA, Modify-Uecontext-Request/Answer</td></tr>
<tr><td>8388723</td><td>BTR/BTA, Background-Data-Transfer-Request/Answer</td></tr>
<tr><td>8388724</td><td>NSR/NSA, Network-Status-Request/Answer</td></tr>
<tr><td>8388725</td><td>NCR/NCA, Network-Status-Continuous-Report-Request/Answer</td></tr>
<tr><td>8388726</td><td>NIR/NIA, NIDD-Information-Request/Answer</td></tr>
<tr><td>8388727</td><td>XAR/XAA, ProXimity-Application-Request/Answer</td></tr>
<tr><td>8388728</td><td>DPR/DPA, Data-Pull-Request/Answer</td></tr>
<tr><td>8388729</td><td>DUR/DUA, Data-Update-Request/Answer</td></tr>
<tr><td>8388730</td><td>NDR/NDA, Notification-Data-Request/Answer</td></tr>
<tr><td>8388731</td><td>TNR/TNA, TSSF-Notification-Request/Answer</td></tr>
<tr><td>8388732</td><td>CMR/CMA, Connection-Management-Request/Answer</td></tr>
<tr><td>8388733</td><td>ODR/ODA, MO-Data-Request/Answer</td></tr>
<tr><td>8388734</td><td>TDR/TDA, MT-Data-Request/Answer</td></tr>
<tr><td>8388735</td><td>ECR/ECA, Event-Configuration-Request/Answer</td></tr>
<tr><td>8388736</td><td>ERR/ERA, Event-Reporting-Request/Answer</td></tr>
</table>
</td></tr>
<tr><td>endToEndId</td><td>String</td><td>O</td><td>The End-to-End Identifier is used to detect duplicate messages.
The data will be extracted from header 'End-to-End' and populated from the first occurrence of the relevant information in the message.</td></tr>
</table>

Table 3-4 (Cont.) Optional xDR Content

<table>
<tr><th>Field Name</th><th>Data Type</th><th>Presence</th><th>Description</th></tr>
<tr><td>resultCode</td><td>String</td><td>O</td><td>Result-Code data field contains the Result Code or Experimental Result values as defined in RFC 3588 (7.1 - 7.7) and TS 29.212 (5.5). Naming convention "E_" signifies the corresponding value is an Experimental-Result code.
It will be populated from the first occurrence of the relevant information in the message and populated from the first occurrence of the relevant information in the message.
The mapped label value will be present in the xDRs, The data will be extracted from either of AVPs:
• Result-Code
• Experimental-Result-Code: In case of expermental-result-code, prefix of '100' is added in value to avoid conflict with the value of Result-Code AVP.
<table>
<tr><th>Value</th><th>Mapped Label</th></tr>
<tr><td>1001</td><td>Diameter multi round auth</td></tr>
<tr><td>2001</td><td>Diameter success</td></tr>
<tr><td>2002</td><td>Diameter limited success</td></tr>
<tr><td>3001</td><td>Diameter command unsupported</td></tr>
<tr><td>3002</td><td>Diameter unable to deliver</td></tr>
<tr><td>3003</td><td>Diameter realm not served</td></tr>
<tr><td>3004</td><td>Diameter too busy</td></tr>
<tr><td>3005</td><td>Diameter loop detected</td></tr>
<tr><td>3006</td><td>Diameter redirect indication</td></tr>
<tr><td>3007</td><td>Diameter application unsupported</td></tr>
<tr><td>3008</td><td>Diameter invalid hdr bits</td></tr>
<tr><td>3009</td><td>Diameter invalid avp bits</td></tr>
<tr><td>3010</td><td>Diameter unknown peer</td></tr>
<tr><td>4001</td><td>Diameter authentication rejected</td></tr>
<tr><td>4002</td><td>Diameter out of space</td></tr>
<tr><td>4003</td><td>Diameter election lost</td></tr>
<tr><td>4010</td><td>Diameter end user service denied</td></tr>
<tr><td>4011</td><td>Diameter credit control not applicable</td></tr>
<tr><td>4012</td><td>Diameter credit limit reached</td></tr>
<tr><td>5001</td><td>Diameter avp unsupported</td></tr>
<tr><td>5002</td><td>Diameter unknown session id</td></tr>
<tr><td>5003</td><td>Diameter authorization rejected</td></tr>
<tr><td>5004</td><td>Diameter invalid avp value</td></tr>
<tr><td>5005</td><td>Diameter missing avp</td></tr>
<tr><td>5006</td><td>Diameter resources exceeded</td></tr>
<tr><td>5007</td><td>Diameter contradicting avps</td></tr>
<tr><td>5008</td><td>Diameter avp not allowed</td></tr>
<tr><td>5009</td><td>Diameter avp occurs too many times</td></tr>
<tr><td>5010</td><td>Diameter no common application</td></tr>
<tr><td>5011</td><td>Diameter unsupported version</td></tr>
<tr><td>5012</td><td>Diameter unable to comply</td></tr>
<tr><td>5013</td><td>Diameter invalid bit in header</td></tr>
<tr><td>5014</td><td>Diameter invalid avp length</td></tr>
</table>
</td></tr>
</table>

Table 3-4 (Cont.) Optional xDR Content

<table>
<tr><th>Field Name</th><th>Data Type</th><th>Presence</th><th>Description</th></tr>
<tr><td></td><td></td><td></td><td>
<table>
<tr><td>5015</td><td>Diameter invalid message length</td></tr>
<tr><td>5016</td><td>Diameter invalid avp bit combo</td></tr>
<tr><td>5017</td><td>Diameter no common security</td></tr>
<tr><td>5030</td><td>Diameter user unknown</td></tr>
<tr><td>5031</td><td>Diameter rating failed</td></tr>
<tr><td>1002001</td><td>Diameter Error First Registration</td></tr>
<tr><td>1002002</td><td>Diameter Error Subsequent Registration</td></tr>
<tr><td>1002003</td><td>Diameter Error Unregistered Service</td></tr>
<tr><td>1002004</td><td>Diameter Error Success Server name Not stored</td></tr>
<tr><td>1002005</td><td>Deprecated Value</td></tr>
<tr><td>1002021</td><td>Diameter Error PDP Context Deletion Indication</td></tr>
<tr><td>1004010</td><td>Diameter Error End User Service Denied</td></tr>
<tr><td>1004011</td><td>Diameter Error Credit Control Not Applicable</td></tr>
<tr><td>1004012</td><td>Diameter Error Credit Limit Reached</td></tr>
<tr><td>1004013</td><td>Diameter Error Customer Not Found</td></tr>
<tr><td>1004100</td><td>Diameter Error User Data Not Available</td></tr>
<tr><td>1004101</td><td>Diameter Error Prior Update In Progress</td></tr>
<tr><td>1004121</td><td>Diameter Error Out of Resources</td></tr>
<tr><td>1004141</td><td>Diameter Error PCC Bearer Event</td></tr>
<tr><td>1004142</td><td>Diameter Error Bearer Event</td></tr>
<tr><td>1004143</td><td>Diameter Error AN GW Failed</td></tr>
<tr><td>1004144</td><td>Diameter Error Pending Transaction</td></tr>
<tr><td>1004181</td><td>Diameter Error Authentication Data Unavailable</td></tr>
<tr><td>1004182</td><td>Diameter Error CAMEL Subscription Present</td></tr>
<tr><td>1004201</td><td>Diameter Error Absent Users</td></tr>
<tr><td>1004221</td><td>Diameter Error Unreachable User</td></tr>
<tr><td>1004222</td><td>Diameter Error Suspended User</td></tr>
<tr><td>1004223</td><td>Diameter Error Detached User</td></tr>
<tr><td>1004224</td><td>Diameter Error Positioning Denied</td></tr>
<tr><td>1004225</td><td>Diameter Error Positioning Failed</td></tr>
<tr><td>1004226</td><td>Diameter Error Unknown Unreachable LCS Client</td></tr>
<tr><td>1004241</td><td>Diameter Error No Available Policy Counters</td></tr>
<tr><td>1005001</td><td>Diameter Error User Unknown</td></tr>
<tr><td>1005002</td><td>Diameter Error Identities Do not Match</td></tr>
<tr><td>1005003</td><td>Diameter Error Identity Not Registered</td></tr>
<tr><td>1005004</td><td>Diameter Error Roaming Not Allowed</td></tr>
</table>
</td></tr>
</table>

Table 3-4 (Cont.) Optional xDR Content

<table>
<tr><th>Field Name</th><th>Data Type</th><th>Presence</th><th>Description</th></tr>
<tr><td></td><td></td><td></td><td>
<table>
<tr><td>1005005</td><td>Diameter Error Identity Already Registered</td></tr>
<tr><td>1005006</td><td>Diameter Error AUTH Scheme Not Supported</td></tr>
<tr><td>1005007</td><td>Diameter Error in Assignment Type</td></tr>
<tr><td>1005008</td><td>Diameter Error Too Much Data</td></tr>
<tr><td>1005009</td><td>Diameter Error Not Supported User Data</td></tr>
<tr><td>1005010</td><td>Unassigned</td></tr>
<tr><td>1005011</td><td>Diameter Error Feature Unsupported</td></tr>
<tr><td>1005012</td><td>Diameter Error serving node feature unsupported</td></tr>
<tr><td>1005030</td><td>Diameter Error user Unknown</td></tr>
<tr><td>1005031</td><td>Diameter Error ratings failed</td></tr>
<tr><td>1005041</td><td>Diameter Error User No WLAN Subscription</td></tr>
<tr><td>1005042</td><td>Diameter Error W-APN Unused By User</td></tr>
<tr><td>1005043</td><td>Diameter Error No Access Independent Subscription</td></tr>
<tr><td>1005044</td><td>Diameter Error User No W-APN Subscription</td></tr>
<tr><td>1005045</td><td>Diameter Error Unsuitable Network</td></tr>
<tr><td>1005061</td><td>Diameter Error Invalid Service Information</td></tr>
<tr><td>1005062</td><td>Diameter Error Filter Restrictions</td></tr>
<tr><td>1005063</td><td>Diameter Error Requested Service Not Authorized</td></tr>
<tr><td>1005064</td><td>Diameter Error Duplicated AF Session</td></tr>
<tr><td>1005065</td><td>Diameter Error IP-CAN Session Not Available</td></tr>
<tr><td>1005066</td><td>Diameter Error Unauthorized Non-Emergency Session</td></tr>
<tr><td>1005067</td><td>Diameter Error Unauthorized Sponsored Data Connectivity</td></tr>
<tr><td>1005068</td><td>Diameter Error Temporary Network Failure</td></tr>
<tr><td>1005100</td><td>Diameter Error User Data Not Recognized</td></tr>
<tr><td>1005101</td><td>Diameter Error Operation Not Allowed</td></tr>
<tr><td>1005102</td><td>Diameter Error User Data Cannot be Read</td></tr>
<tr><td>1005103</td><td>Diameter Error User Data Cannot be Modified</td></tr>
<tr><td>1005104</td><td>Diameter Error User Data Cannot be Notified</td></tr>
<tr><td>1005105</td><td>Diameter Error Transparent Data Out of Sync</td></tr>
<tr><td>1005106</td><td>Diameter Error Subs Data Absent</td></tr>
</table>
</td></tr>
</table>

Table 3-4 (Cont.) Optional xDR Content

<table>
<tr><th>Field Name</th><th>Data Type</th><th>Presence</th><th>Description</th></tr>
<tr><td></td><td></td><td></td><td>
<table>
<tr><td>1005107</td><td>Diameter Error No Subscription to data</td></tr>
<tr><td>1005108</td><td>Diameter Error DSAI Not Available</td></tr>
<tr><td>1005120</td><td>Diameter Error Start Indication</td></tr>
<tr><td>1005121</td><td>Diameter Error Stop Indication</td></tr>
<tr><td>1005122</td><td>Diameter Error Unknown MBMS Bearer Service</td></tr>
<tr><td>1005123</td><td>Diameter Error Service Area</td></tr>
<tr><td>1005140</td><td>Diameter Error Initial Parameters</td></tr>
<tr><td>1005141</td><td>Diameter Error Trigger Event</td></tr>
<tr><td>1005142</td><td>Diameter Error PCC Rule Event</td></tr>
<tr><td>1005143</td><td>Diameter Error Bearer Not Authorized</td></tr>
<tr><td>1005144</td><td>Diameter Error Traffic Mapping Info Rejected</td></tr>
<tr><td>1005145</td><td>Diameter Error QOS Rule Event</td></tr>
<tr><td>1005146</td><td>Reserved</td></tr>
<tr><td>1005147</td><td>Diameter Error Conflicting Request</td></tr>
<tr><td>1005148</td><td>Diameter Error ADC Rule Event</td></tr>
<tr><td>1005401</td><td>Diameter Error IMPI Unknown</td></tr>
<tr><td>1005402</td><td>Diameter Error Not Authorized</td></tr>
<tr><td>1005403</td><td>Diameter Error Transaction Identifier Invalid</td></tr>
<tr><td>1005404</td><td>Reserved Experimental Result Code</td></tr>
<tr><td>1005405</td><td>Diameter Error Identity Unknown</td></tr>
<tr><td>1005420</td><td>Diameter Error Unknown EPS Subscription</td></tr>
<tr><td>1005421</td><td>Diameter Error RAT Not Allowed</td></tr>
<tr><td>1005422</td><td>Diameter Error Equipment Unknown</td></tr>
<tr><td>1005423</td><td>Diameter Error Unknown Serving Node</td></tr>
<tr><td>1005450</td><td>Diameter Error User No NON 3GPP Subscription</td></tr>
<tr><td>1005451</td><td>Diameter Error User No APN Subscription</td></tr>
<tr><td>1005452</td><td>Diameter Error RAT Type Not Allowed</td></tr>
<tr><td>1005470</td><td>Diameter Error Sub-Session</td></tr>
<tr><td>1005471</td><td>Diameter Error Ongoing Session Establishment</td></tr>
<tr><td>1005490</td><td>Diameter Error Unauthorized Requesting Network</td></tr>
<tr><td>1005510</td><td>Diameter Error Unauthorized Requesting Entity</td></tr>
<tr><td>1005511</td><td>Diameter Error Unauthorized Service</td></tr>
<tr><td>1005530</td><td>Diameter Error Invalid SME Address</td></tr>
<tr><td>1005531</td><td>Diameter Error SC Congestion</td></tr>
<tr><td>1005532</td><td>Diameter Error SM Protocol</td></tr>
<tr><td>1005533</td><td>Diameter Error Trigger Replace Failure</td></tr>
</table>
</td></tr>
</table>

Table 3-4 (Cont.) Optional xDR Content

<table>
<tr><th>Field Name</th><th>Data Type</th><th>Presence</th><th>Description</th></tr>
<tr><td></td><td></td><td></td><td>
<table>
<tr><td>1005534</td><td>Diameter Error Trigger Recall Failure</td></tr>
<tr><td>1005535</td><td>Diameter Error Original Message Not Pending</td></tr>
<tr><td>1005550</td><td>Diameter Error Absent User</td></tr>
<tr><td>1005551</td><td>Diameter Error User Busy For MT SMS</td></tr>
<tr><td>1005552</td><td>Diameter Error Facility Not Supported</td></tr>
<tr><td>1005553</td><td>Diameter Error Illegal User</td></tr>
<tr><td>1005554</td><td>Diameter Error Illegal Equipment</td></tr>
<tr><td>1005555</td><td>Diameter Error SM Delivery Failure</td></tr>
<tr><td>1005556</td><td>Diameter Error Service Not Subscribed</td></tr>
<tr><td>1005557</td><td>Diameter Error Service Barred</td></tr>
<tr><td>1005558</td><td>Diameter Error MWD List Full</td></tr>
<tr><td>1005570</td><td>Diameter Error Unknown Policy Counters</td></tr>
</table>
</td></tr>
<tr><td>sessionId</td><td>String</td><td>O</td><td>A session is a logical concept at the application layer, and is shared between an access device and a server, and is identified via the Session-Id.
The data will be extracted from AVP 'Session-Id' and populated from the first occurrence of the relevant information in the message.</td></tr>
<tr><td>originHost</td><td>String</td><td>O</td><td>It identifies the endpoint that originated the Diameter message.
The data will be extracted from AVP 'Origin-Host' and populated from the first occurrence of the relevant information in the message.</td></tr>
<tr><td>originRealm</td><td>String</td><td>O</td><td>Origin Domain of the request message.
The data will be extracted from AVP 'Origin-Realm' and populated from the first occurrence of the relevant information in the message.</td></tr>
<tr><td>destinationHost</td><td>String</td><td>O</td><td>It identifies the endpoint to which the Diameter message is intended.
The data will be extracted from AVP 'Destination-Host' and populated from the first occurrence of the relevant information in the message.</td></tr>
<tr><td>destinationRealm</td><td>String</td><td>O</td><td>Destination Realm contains the realm the message is to be routed to.
The data will be extracted from AVP 'Destination-Realm' and populated from the first occurrence of the relevant information in the message.</td></tr>
<tr><td>imsi</td><td>String</td><td>O</td><td>The International Mobile Subscriber Identity (IMSI) is a unique number associated with a mobile phone user. It's used to identify a subscriber to a cellular network.
The data will be extracted from following AVP and populated from the first occurrence of the relevant information in the message.
<table>
<tr><th>AVP-NAME with Order</th></tr>
<tr><td>Subscription-Id-Data
(END_USER_IMSI, END_USER_SIP_URI)</td></tr>
<tr><td>User-Name</td></tr>
<tr><td>3GPP-IMSI</td></tr>
<tr><td>3GPP-IMSI-MCC-MNC</td></tr>
</table>
</td></tr>
</table>

Table 3-4 (Cont.) Optional xDR Content

Field Name	Data Type	Presence	Description
msisdn	String	O	The Mobile Station International Subscriber Directory Number (MSISDN) is a unique number assigned to a mobile phone subscriber. It's essentially the phone number associated with a SIM card or mobile device. The data will be extracted from following AVP and populated from the first occurrence of the relevant information in the message. **AVP-NAME with Order** Subscription-Id-Data (END_USER_MSISDN,END_USER_SIP_URI) MSISDN A-MSISDN
impu	String	O	It contains the public identity of a user. The data will be extracted from following AVP and populated from the first occurrence of the relevant information in the message. **AVP-NAME with Order** Public-Identity Wildcarded-IMPU Wildcarded-Public-Identity
impi	String	O	It contains the private identity of a user. The data will be extracted from AVP 'User-Name' and populated from the first occurrence of the relevant information in the message.
routeRecord	String	O	It contains the route-record field of the message. The data will be extracted from AVP 'Route-Record' and populated from the last occurrence of the relevant information in the message.
vendorId	String	O	It contains the Vendor Id extracted from 'Vendor-Id' AVP present inside Grouped AVP 'Vendor-Specific-Application-Id'. It populated from the first occurrence of the relevant information in the message.

Table 3-4 (Cont.) Optional xDR Content

<table>
<tr><th>Field Name</th><th>Data Type</th><th>Presence</th><th>Description</th></tr>
<tr><td>authApplicationId</td><td>String</td><td>O</td><td>It contains the Authentication Application Id extracted from the Auth-Application-Id AVP.
The data will be extracted from AVP 'Auth-Application-Id' and populated from the last occurrence of the relevant information in the message.
The mapped label value will be present in the xDRs.
<table>
<tr><th>Value</th><th>Mapped Label</th></tr>
<tr><td>0</td><td>Diameter Common</td></tr>
<tr><td>16777236</td><td>Rx</td></tr>
<tr><td>16777217</td><td>Sh</td></tr>
<tr><td>16777238</td><td>Gx</td></tr>
<tr><td>16777251</td><td>S6a/S6d</td></tr>
<tr><td>16777252</td><td>S13</td></tr>
<tr><td>16777272</td><td>S6b</td></tr>
<tr><td>16777251</td><td>S6</td></tr>
<tr><td>16777252</td><td>S13</td></tr>
<tr><td>16777216</td><td>Cx</td></tr>
<tr><td>16777255</td><td>SLg</td></tr>
<tr><td>16777291</td><td>SLh</td></tr>
<tr><td>16777303</td><td>Sd</td></tr>
<tr><td>16777265</td><td>SWx</td></tr>
</table></td></tr>
<tr><td>subscriberStatus</td><td>String</td><td>O</td><td>It indicates the current status of a subscriber. it is typically used in User-Data-Request (UDR) and User-Data-Answer (UDA) diameter messages.
The data will be extracted from AVP 'Subscriber-Status' and populated from the last occurrence of the relevant information in the message.</td></tr>
</table>

Table 3-4 (Cont.) Optional xDR Content

<table>
<tr><th>Field Name</th><th>Data Type</th><th>Presence</th><th>Description</th></tr>
<tr><td>ratType</td><td>String</td><td>O</td><td>It indicates which Radio Access Technology is currently serving the UE. To differentiate between RAT-Type and 3GPP-RAT-Type AVPs "(3GPP)" has been introduced in the names.
The data will be extracted from AVP 'RAT-Type' and populated from the last occurrence of the relevant information in the message.
The mapped label value will be present in the xDRs.
<table>
<tr><th>Value</th><th>Mapped Label</th></tr>
<tr><td>0</td><td>WLAN</td></tr>
<tr><td>1</td><td>UTRAN(3GPP)</td></tr>
<tr><td>2</td><td>GERAN(3GPP)</td></tr>
<tr><td>3</td><td>WLAN(3GPP)</td></tr>
<tr><td>4</td><td>GAN(3GPP)</td></tr>
<tr><td>5</td><td>HSPA Evolution(3GPP)</td></tr>
<tr><td>6</td><td>EUTRAN(3GPP)</td></tr>
<tr><td>7</td><td>VIRTUAL</td></tr>
<tr><td>101</td><td>IEEE 802.16e(3GPP)</td></tr>
<tr><td>102</td><td>3GPP2 eHRPD(3GPP)</td></tr>
<tr><td>103</td><td>3GPP2 HRPD(3GPP)</td></tr>
<tr><td>104</td><td>3GPP2 1xRTT(3GPP)</td></tr>
<tr><td>105</td><td>3GPP2 UMB</td></tr>
<tr><td>1000</td><td>UTRAN</td></tr>
<tr><td>1001</td><td>GERAN</td></tr>
<tr><td>1002</td><td>GAN</td></tr>
<tr><td>1003</td><td>HSPA_EVOLUTION</td></tr>
<tr><td>1004</td><td>EUTRAN</td></tr>
<tr><td>2000</td><td>CDMA2000_1X</td></tr>
<tr><td>2001</td><td>HRPD</td></tr>
<tr><td>2002</td><td>UMB</td></tr>
<tr><td>2003</td><td>EHRPD</td></tr>
</table></td></tr>
<tr><td>visitedPlmnId</td><td>String</td><td>O</td><td>It refers to the identifier of the Public Land Mobile Network (PLMN) that a mobile device is currently visiting or connected to.
The data will be extracted from AVP 'Visited-PLMN-Id and populated from the last occurrence of the relevant information in the message.</td></tr>
<tr><td>userLocationInfo3gpp</td><td>String</td><td>O</td><td>It refers to information related to the location of a user in a 3GPP (3rd Generation Partnership Project) network
The data will be extracted from AVP '3GPP-User-Location-Info' and populated from the last occurrence of the relevant information in the message.</td></tr>
</table>

Table 3-4 (Cont.) Optional xDR Content

<table>
<tr><th>Field Name</th><th>Data Type</th><th>Presence</th><th>Description</th></tr>
<tr><td>qosClassIdentifier</td><td>String</td><td>O</td><td>It used in cellular networks to identify the Quality of Service (QoS) characteristics of a data flow or a service.
The data will be extracted from AVP 'QoS-Class-Identifier' and populated from the last occurrence of the relevant information in the message.
The mapped label value will be present in the xDRs.
<table>
<tr><th>Value</th><th>Mapped Label</th></tr>
<tr><td>1</td><td>QCI_1</td></tr>
<tr><td>2</td><td>QCI_2</td></tr>
<tr><td>3</td><td>QCI_3</td></tr>
<tr><td>4</td><td>QCI_4</td></tr>
<tr><td>5</td><td>QCI_5</td></tr>
<tr><td>6</td><td>QCI_6</td></tr>
<tr><td>7</td><td>QCI_7</td></tr>
<tr><td>8</td><td>QCI_8</td></tr>
<tr><td>9</td><td>QCI_9</td></tr>
<tr><td>65</td><td>QCI_65</td></tr>
<tr><td>66</td><td>QCI_66</td></tr>
<tr><td>67</td><td>QCI_67</td></tr>
<tr><td>69</td><td>QCI_69</td></tr>
<tr><td>70</td><td>QCI_70</td></tr>
<tr><td>71</td><td>QCI_71</td></tr>
<tr><td>72</td><td>QCI_72</td></tr>
<tr><td>73</td><td>QCI_73</td></tr>
<tr><td>74</td><td>QCI_74</td></tr>
<tr><td>75</td><td>QCI_75</td></tr>
<tr><td>76</td><td>QCI_76</td></tr>
<tr><td>79</td><td>QCI_79</td></tr>
<tr><td>80</td><td>QCI_80</td></tr>
<tr><td>82</td><td>QCI_82</td></tr>
<tr><td>83</td><td>QCI_83</td></tr>
<tr><td>84</td><td>QCI_84</td></tr>
<tr><td>85</td><td>QCI_85</td></tr>
</table></td></tr>
<tr><td>cancellationType</td><td>String</td><td>O</td><td>Cancellation type defined in cancel Location.
The data will be extracted from AVP 'Cancellation-Type' and populated from the last occurrence of the relevant information in the message.
The mapped label value will be present in the xDRs.
<table>
<tr><th>Value</th><th>Mapped Label</th></tr>
<tr><td>0</td><td>MME Update Procedure</td></tr>
<tr><td>1</td><td>SGSN Update Procedure</td></tr>
<tr><td>2</td><td>Subscription Withdrawal</td></tr>
<tr><td>3</td><td>Update Procedure IWF</td></tr>
<tr><td>4</td><td>Initial Attach Procedure</td></tr>
</table></td></tr>
</table>

Table 3-4 (Cont.) Optional xDR Content

<table>
<tr><th>Field Name</th><th>Data Type</th><th>Presence</th><th>Description</th></tr>
<tr><td>addrType</td><td>String</td><td>O</td><td>This field indicates the Address Type come in IP source and Destination Address is either IPv4 or IPv6 format.
The data will be extracted from AVP '' and populated from the first occurrence of the relevant information in the message.
The mapped label value will be present in the xDRs.
<table>
<tr><th>Value</th><th>Mapped Label</th></tr>
<tr><td>0x04</td><td>IP_V4</td></tr>
<tr><td>0x06</td><td>IP_V6</td></tr>
</table></td></tr>
<tr><td>accApplicationId</td><td>String</td><td>O</td><td>It contains the Accounting Application Id extracted from the Acct-Application-Id AVP.
The data will be extracted from AVP 'Acct-Application-Id' and populated from the first occurrence of the relevant information in the message.
The mapped label value will be present in the xDRs.
<table>
<tr><th>Value</th><th>Mapped Label</th></tr>
<tr><td>0</td><td>Diameter Common</td></tr>
<tr><td>16777251</td><td>S6a/S6d</td></tr>
<tr><td>16777252</td><td>S13</td></tr>
<tr><td>16777272</td><td>S6b</td></tr>
<tr><td>16777236</td><td>Rx</td></tr>
<tr><td>16777238</td><td>Gx</td></tr>
</table></td></tr>
<tr><td>reqHeaderFlag</td><td>String</td><td>O</td><td>It contains the Request flag coming in Diameter header.
The data will be extracted from request message header 'Flags' and populated from the first occurrence of the relevant information in the message.
The mapped label value will be present in the xDRs.
<table>
<tr><th>Value</th><th>Mapped Label</th></tr>
<tr><td>0x80</td><td>Request</td></tr>
<tr><td>0x90</td><td>Request, T bit set</td></tr>
<tr><td>0xa0</td><td>Request, E bit set</td></tr>
<tr><td>0xb0</td><td>Request, E, T bit set</td></tr>
<tr><td>0xc0</td><td>Request,P bit set</td></tr>
<tr><td>0xd0</td><td>Request, P, T bit set</td></tr>
<tr><td>0xe0</td><td>Request, P, E bit set</td></tr>
<tr><td>0xf0</td><td>Request, P, E, T bit set</td></tr>
</table></td></tr>
</table>

Table 3-4 (Cont.) Optional xDR Content

<table>
<tr><th>Field Name</th><th>Data Type</th><th>Presence</th><th>Description</th></tr>
<tr><td>ansHeaderFlag</td><td>String</td><td>O</td><td>It contains the Response flag coming in Diameter header.
The data will be extracted from response message header 'Flags' and populated from the first occurrence of the relevant information in the message.
The mapped label value will be present in the xDRs.
<table>
<tr><th>Value</th><th>Mapped Label</th></tr>
<tr><td>0x00</td><td>Answer</td></tr>
<tr><td>0x10</td><td>Answer, T bit set</td></tr>
<tr><td>0x20</td><td>Answer, E bit set</td></tr>
<tr><td>0x40</td><td>Answer, P bit set</td></tr>
<tr><td>0x50</td><td>Answer, P, T bit set</td></tr>
<tr><td>0x60</td><td>Answer, P, E bit set</td></tr>
<tr><td>0x70</td><td>Answer, P, E, T bit set</td></tr>
</table></td></tr>
<tr><td>equipmentStatus</td><td>String</td><td>O</td><td>Equipment Status extracted from ME-identity-Check-Answer AVP.
The data will be extracted from AVP 'Equipment-Status' and populated from the first occurrence of the relevant information in the message.
The mapped label value will be present in the xDRs.
<table>
<tr><th>Value</th><th>Mapped Label</th></tr>
<tr><td>0</td><td>White Listed</td></tr>
<tr><td>1</td><td>Black Listed</td></tr>
<tr><td>2</td><td>Grey Listed</td></tr>
</table></td></tr>
<tr><td>alertReason</td><td>String</td><td>O</td><td>It indicates the reason for the alert message.
The data will be extracted from AVP 'Alert-Reaosn' and populated from the first occurrence of the relevant information in the message.
The mapped label value will be present in the xDRs.
<table>
<tr><th>Value</th><th>Mapped Label</th></tr>
<tr><td>0</td><td>UE_PRESENT</td></tr>
<tr><td>1</td><td>UE_MEMORY_AVAILABLE</td></tr>
</table></td></tr>
<tr><td>sgsnNumber</td><td>String</td><td>O</td><td>ISDN number of the SGSN.
The data will be extracted from AVP 'SGSN-Number' and populated from the first occurrence of the relevant information in the message.</td></tr>
<tr><td>terminalInfo</td><td>String</td><td>O</td><td>IMEI of the user equipment, It refers to information related to a mobile device or terminal, such as a smartphone, tablet, or other cellular-enabled device
The data will be extracted from AVP 'IMEI' which is present inside Terminal-Information and populated from the first occurrence of the relevant information in the message.</td></tr>
<tr><td>featureList</td><td>String</td><td>O</td><td>List of supported features of the Origin Host.
The data will be extracted from AVP 'Feature-List' and populated from the first occurrence of the relevant information in the message.</td></tr>
</table>

Table 3-4 (Cont.) Optional xDR Content

<table>
<tr><th>Field Name</th><th>Data Type</th><th>Presence</th><th>Description</th></tr>
<tr><td>serviceSelection</td><td>String</td><td>O</td><td>It indicates the name of the service or external network with which the mobility service should be associate.
The data will be extracted from AVP 'Service-Selection' and populated from the first occurrence of the relevant information in the message.</td></tr>
<tr><td>userId</td><td>String</td><td>O</td><td>It contains the leading digits of an IMSI formatted as a character string. It identifies a set of subscribers. Each with identical leading IMSI digits.
The data will be extracted from AVP 'User-Id' and populated from the first occurrence of the relevant information in the message.</td></tr>
<tr><td>mIPHomeAgentAddrType</td><td>String</td><td>O</td><td>This field indicates the Address Type comes in MIP Home Agent Address AVP is either IPv4 or IPv6 format.
The data will be extracted from AVP 'Mip-Home-Agent-Addr-Type' and populated from the first occurrence of the relevant information in the message.
The mapped label value will be present in the xDRs.<table><tr><th>Value</th><th>Mapped Label</th></tr><tr><td>0x04</td><td>IP_V4</td></tr><tr><td>0x06</td><td>IP_V6</td></tr></table></td></tr>
<tr><td>mIPHomeAgentHost</td><td>String</td><td>O</td><td>It refers to the hostname or Fully Qualified Domain Name (FQDN) of a Mobile IP Home Agent (HA).
The data will be extracted from AVP 'Destination-Host' which is present inside MIP-Home-Agent-Host and populated from the first occurrence of the relevant information in the message.</td></tr>
<tr><td>mIPHomeAgentAddress</td><td>String</td><td>O</td><td>It refers to the IP address of a Mobile IP Home Agent (HA) in a Mobile IP network.
The data will be extracted from AVP 'MIP-Home-Agent-Address' and populated from the first occurrence of the relevant information in the message.</td></tr>
<tr><td>mIPHomeAgentRealm</td><td>String</td><td>O</td><td>It refers to the realm or domain associated with a Mobile IP Home Agent (HA).
The data will be extracted from AVP 'Destination-Realm' which is present inside MIP-Home-Agent-Host and populated from the first occurrence of the relevant information in the message.</td></tr>
<tr><td>networkAccessMode</td><td>String</td><td>O</td><td>This field indicates whether the traffic is Packet or Circuit or combination of both.
The data will be extracted from AVP 'Network-Access-Mode' and populated from the first occurrence of the relevant information in the message.
The mapped label value will be present in the xDRs.<table><tr><th>Value</th><th>Mapped Label</th></tr><tr><td>0</td><td>Packet and Circuit</td></tr><tr><td>1</td><td>Reserved</td></tr><tr><td>2</td><td>Only Packet</td></tr></table></td></tr>
</table>

Table 3-4 (Cont.) Optional xDR Content

<table>
<tr><th>Field Name</th><th>Data Type</th><th>Presence</th><th>Description</th></tr>
<tr><td>visitedNetworkId</td><td>String</td><td>O</td><td>It refers to an identifier that represents the visited network that a user is currently connected to.
The data will be extracted from AVP 'Visited-Network-Identifier' and populated from the first occurrence of the relevant information in the message.</td></tr>
<tr><td>requestCause</td><td>String</td><td>O</td><td>It contains the reason for sending the credit-control request message. It must be present in all Credit-Control-Request messages.
The data will be extracted from AVP 'CC-Request-Type' and populated from the first occurrence of the relevant information in the message.
The mapped label value will be present in the xDRs.
<table>
<tr><th>Value</th><th>Mapped Label</th></tr>
<tr><td>1</td><td>Initial Request</td></tr>
<tr><td>2</td><td>Update Request</td></tr>
<tr><td>3</td><td>Termination Request</td></tr>
<tr><td>4</td><td>Event Request</td></tr>
</table></td></tr>
<tr><td>terminationCause</td><td>String</td><td>O</td><td>It contains the reason the credit control session terminated.
The data will be extracted from AVP 'Termination-Cause' and populated from the first occurrence of the relevant information in the message.
The mapped label value will be present in the xDRs.
<table>
<tr><th>Value</th><th>Mapped Label</th></tr>
<tr><td>1</td><td>Diameter Logout</td></tr>
<tr><td>2</td><td>Diameter Service Not Provided</td></tr>
<tr><td>3</td><td>Diameter Bad Answer</td></tr>
<tr><td>4</td><td>Diameter Administrative</td></tr>
<tr><td>5</td><td>Diameter Link Broken</td></tr>
<tr><td>6</td><td>Diameter Auth Expired</td></tr>
<tr><td>7</td><td>Diameter User Moved</td></tr>
<tr><td>8</td><td>Diameter Session Timeout</td></tr>
</table></td></tr>
<tr><td>reAuthRequestType</td><td>String</td><td>O</td><td>It contains the action expected upon expiration of the Authorization-Lifetime.It must be present in Re-auth answer message if message contains a positive value for Authorization-Lifetime.
The data will be extracted from AVP 'Re-Auth-Request-Type' and populated from the first occurrence of the relevant information in the message.
The mapped label value will be present in the xDRs.
<table>
<tr><th>Value</th><th>Mapped Label</th></tr>
<tr><td>0</td><td>AUTHORIZE_ONLY</td></tr>
<tr><td>1</td><td>AUTHORIZE_AUTHENTICATE</td></tr>
</table></td></tr>
</table>

Table 3-4 (Cont.) Optional xDR Content

<table>
<tr><th>Field Name</th><th>Data Type</th><th>Presence</th><th>Description</th></tr>
<tr><td>eventTrigger</td><td>String</td><td>O</td><td>It indicates the triggered event sent by PCEF to PCRF as part of Event-Report-Indication AVP.For each of the values mentioned below, the corresponding bit of this field is set.
The data will be extracted from AVP 'Event-Trigger' and populated from the first occurrence of the relevant information in the message.
The mapped label value will be present in the xDRs.
<table>
<tr><th>Value</th><th>Mapped Label</th></tr>
<tr><td>0</td><td>SGSN_CHANGE</td></tr>
<tr><td>1</td><td>QOS_CHANGE</td></tr>
<tr><td>2</td><td>RAT_CHANGE</td></tr>
<tr><td>3</td><td>TFT_CHANGE</td></tr>
<tr><td>4</td><td>PLMN_CHANGE</td></tr>
<tr><td>5</td><td>LOSS_OF_BEARER</td></tr>
<tr><td>6</td><td>RECOVERY_OF_BEARER</td></tr>
<tr><td>7</td><td>IP_CAN_CHANGE</td></tr>
<tr><td>11</td><td>QOS_CHANGE_EXCEEDING_AUTHORIZATION</td></tr>
<tr><td>12</td><td>RAI_CHANGE</td></tr>
<tr><td>13</td><td>USER_LOCATION_CHANGE</td></tr>
<tr><td>14</td><td>NO_EVENT_TRIGGERS</td></tr>
<tr><td>15</td><td>OUT_OF_CREDIT</td></tr>
<tr><td>16</td><td>REALLOCATION_OF_CREDIT</td></tr>
<tr><td>17</td><td>REVALIDATION_TIMEOUT</td></tr>
<tr><td>18</td><td>UE_IP_ADDRESS_ALLOCATE</td></tr>
<tr><td>19</td><td>UE_IP_ADDRESS_RELEASE</td></tr>
<tr><td>20</td><td>DEFAULT_EPS_BEARER_QOS_CHANGE</td></tr>
<tr><td>21</td><td>AN_GW_CHANGE</td></tr>
<tr><td>22</td><td>SUCCESSFUL_RESOURCE_ALLOCATION</td></tr>
<tr><td>23</td><td>RESOURCE_MODIFICATION_REQUEST</td></tr>
<tr><td>24</td><td>PGW_TRACE_CONTROL</td></tr>
<tr><td>25</td><td>UE_TIME_ZONE_CHANGE</td></tr>
<tr><td>26</td><td>TAI_CHANGE</td></tr>
<tr><td>27</td><td>ECGI_CHANGE</td></tr>
<tr><td>28</td><td>CHARGING_CORRELATION_EXCHANGE</td></tr>
<tr><td>29</td><td>APN-AMBR_MODIFICATION_FAILURE</td></tr>
<tr><td>30</td><td>USER_CSG_INFORMATION_CHANGE</td></tr>
<tr><td>33</td><td>USAGE_REPORT</td></tr>
<tr><td>34</td><td>DEFAULT-EPS-BEARER-QOS_MODIFICATION_FAILURE</td></tr>
<tr><td>35</td><td>USER_CSG_HYBRID_SUBSCRIBED_INFORMATION_CHANGE</td></tr>
</table>
</td></tr>
</table>

Table 3-4 (Cont.) Optional xDR Content

<table>
<tr><th>Field Name</th><th>Data Type</th><th>Presence</th><th>Description</th></tr>
<tr><td></td><td></td><td></td><td>
<table>
<tr><td>36</td><td>USER_CSG_HYBRID_UNSUBSCRIBED_INFORMATION_CHANGE</td></tr>
<tr><td>37</td><td>ROUTING_RULE_CHANGE</td></tr>
<tr><td>39</td><td>APPLICATION_START</td></tr>
<tr><td>40</td><td>APPLICATION_STOP</td></tr>
<tr><td>42</td><td>CS_TO_PS_HANDOVER</td></tr>
<tr><td>43</td><td>UE_LOCAL_IP_ADDRESS_CHANGE</td></tr>
<tr><td>44</td><td>H(E)NB_LOCAL_IP_ADDRESS_CHANGE</td></tr>
<tr><td>45</td><td>ACCESS_NETWORK_INFO_REPORT</td></tr>
<tr><td>46</td><td>CREDIT_MANAGEMENT_SESSION_FAILURE</td></tr>
<tr><td>47</td><td>DEFAULT_QOS_CHANGE</td></tr>
<tr><td>48</td><td>CHANGE_OF_UE_PRESENCE_IN_PRESENCE_REPORTING_AREA_REPORT</td></tr>
<tr><td>49</td><td>ADDITION_OF_ACCESS</td></tr>
<tr><td>50</td><td>REMOVAL_OF_ACCESS</td></tr>
<tr><td>51</td><td>UNAVAILABLITY_OF_ACCESS</td></tr>
<tr><td>52</td><td>AVAILABLITY_OF_ACCESS</td></tr>
<tr><td>53</td><td>RESOURCE_RELEASE</td></tr>
<tr><td>54</td><td>ENODEB_CHANGE</td></tr>
<tr><td>55</td><td>3GPP_PS_DATA_OFF_CHANGE</td></tr>
<tr><td>56</td><td>UE_STATUS_RESUME</td></tr>
<tr><td>57</td><td>SUCCESSFUL_QOS_UPDATE</td></tr>
</table>
</td></tr>
<tr><td>sessionReleaseCause</td><td>String</td><td>O</td><td>It determines the cause of release the IP-CAN session by the PCRF.
The data will be extracted from AVP 'Session-Release-Cause' and populated from the first occurrence of the relevant information in the message.
The mapped label value will be present in the xDRs.
<table>
<tr><th>Value</th><th>Mapped Label</th></tr>
<tr><td>0</td><td>UNSPECIFIED_REASON</td></tr>
<tr><td>1</td><td>UE_SUBSCRIPTION_REASON</td></tr>
<tr><td>2</td><td>INSUFFICIENT_SERVER_RESOURCES</td></tr>
<tr><td>3</td><td>IP_CAN_SESSION_TERMINATION</td></tr>
<tr><td>4</td><td>UE_IP_ADDRESS_RELEASE</td></tr>
</table>
</td></tr>
<tr><td>priorityLevel</td><td>String</td><td>O</td><td>Defines the relative importance of a resource request.
The data will be extracted from AVP 'Priority-Level' and populated from the first occurrence of the relevant information in the message.</td></tr>
</table>

Table 3-4 (Cont.) Optional xDR Content

<table>
<tr><th>Field Name</th><th>Data Type</th><th>Presence</th><th>Description</th></tr>
<tr><td>ipCanType</td><td>String</td><td>O</td><td>It indicates the type of Connectivity Access Network in which the user is connected.It indicates the type of Connectivity Access Network in which the user is connected.
The data will be extracted from AVP 'IP-CAN-Type' and populated from the first occurrence of the relevant information in the message.
The mapped label value will be present in the xDRs.
<table>
<tr><th>Value</th><th>Mapped Label</th></tr>
<tr><td>0</td><td>3GPP-GPRS</td></tr>
<tr><td>1</td><td>DOCSIS</td></tr>
<tr><td>2</td><td>xDSL</td></tr>
<tr><td>3</td><td>WiMax</td></tr>
<tr><td>4</td><td>3GPP2</td></tr>
<tr><td>5</td><td>3GPP-EPS</td></tr>
<tr><td>6</td><td>Non-3GPP-EPS</td></tr>
<tr><td>7</td><td>FBA</td></tr>
<tr><td>8</td><td>3GPP-5GS</td></tr>
<tr><td>9</td><td>Non-3GPP-5GS</td></tr>
</table></td></tr>
<tr><td>pdnType</td><td>String</td><td>O</td><td>It indicates the IP Address Type (IPv4 or IPv6) of the PDN.
The data will be extracted from AVP 'PDN-Type' and populated from the first occurrence of the relevant information in the message.
The mapped label value will be present in the xDRs.
<table>
<tr><th>Value</th><th>Mapped Label</th></tr>
<tr><td>0</td><td>IPv4</td></tr>
<tr><td>1</td><td>IPv4</td></tr>
<tr><td>2</td><td>IPv4v6</td></tr>
<tr><td>3</td><td>IPv4_OR_IPv6</td></tr>
</table></td></tr>
<tr><td>locationType</td><td>STRING</td><td>0</td><td>To identify Cell Identity or Service area code or Routing area code where the MS is currently located for a given MNC and LAC
The data will be extracted from 1st byte(Geographic Location Type) of AVP '3GPP-User-Location-Info' and populated from the first occurrence of the relevant information in the message.
The mapped label value will be present in the xDRs.
<table>
<tr><th>Value</th><th>Mapped Label</th></tr>
<tr><td>0</td><td>CGI</td></tr>
<tr><td>1</td><td>SAI</td></tr>
<tr><td>2</td><td>RAI</td></tr>
<tr><td>128</td><td>TAI</td></tr>
<tr><td>129</td><td>ECGI</td></tr>
<tr><td>130</td><td>TAI and ECGI</td></tr>
</table></td></tr>
</table>

Table 3-4 (Cont.) Optional xDR Content

Field Name	Data Type	Presence	Description
mcc	String	O	It refers to the Mobile Country Code, a 3-digit code that identifies the country where a mobile network is located SIP_URI, The data will be extracted from AVP '3GPP-Uset-Location-Info' and populated from the last occurrence of the relevant information in the message. From AVP: 3GPP-User-Location-Info **AVP-NAME with Order** Cell-Global-Identity Service-Area-Identity Routing-Area-Identity Tracking-Area-Identity E-UTRAN-Cell-Global-Identity
mnc	String	O	It refers to the Mobile Network Code, a code that identifies a specific mobile network operator within a country or region. The data will be extracted from AVP '' and populated from the last occurrence of the relevant information in the message. From AVP: 3GPP-User-Location-Info **AVP-NAME with Order** Cell-Global-Identity Service-Area-Identity Routing-Area-Identity Tracking-Area-Identity E-UTRAN-Cell-Global-Identity
eci	String	O	It refers to the E-UTRAN Cell Global Identifier (ECGI), which is a unique identifier for a cell in an Evolved Universal Terrestrial Radio Access Network (E-UTRAN). The data will be extracted from "EUTRAN Cell Global Identifier" present in AVP '3GPP-User-Location-Info' and populated from the last occurrence of the relevant information in the message.
lac	String	O	It refers to the Location Area Code, a unique identifier used in cellular networks to identify a group of cells within a network. The data will be extracted from AVP '3GPP-User-Location-Info' and populated from the last occurrence of the relevant information in the message. From AVP: 3GPP-User-Location-Info **AVP-NAME with Order** Cell-Global-Identity Service-Area-Identity Routing-Area-Identity

Table 3-4 (Cont.) Optional xDR Content

<table>
<tr><th>Field Name</th><th>Data Type</th><th>Presence</th><th>Description</th></tr>
<tr><td>sac</td><td>String</td><td>O</td><td>Service area code or Routing area code where the MS is currently located, for a given (MNC, LAC).
The data will be extracted from "Service Area Identifier" present in AVP '3GPP-User-Location-Info' and populated from the last occurrence of the relevant information in the message.</td></tr>
<tr><td>tac</td><td>String</td><td>O</td><td>Tracking Area Code of where the MS is currently located, for a given (MNC).
The data will be extracted from "Tracking Area Identifier" present in AVP '3GPP-User-Location-Info' and populated from the last occurrence of the relevant information in the message.</td></tr>
<tr><td>cellId</td><td>String</td><td>O</td><td>It refers to the Cell Identity, a unique identifier for a cell within a cellular network.
The data will be extracted from "Cell Global Identifier" present in AVP '3GPP-User-Location-Info' and populated from the last occurrence of the relevant information in the message.</td></tr>
<tr><td>sgsnMccMnc</td><td>String</td><td>O</td><td>It refers to a parameter that contains the Mobile Country Code (MCC) and Mobile Network Code (MNC) of the Serving GPRS Support Node (SGSN) in a 3GPP (3rd Generation Partnership Project) network.
The data will be extracted from AVP '3GPP-SGSN-MCC-MNC' and populated from the last occurrence of the relevant information in the message.</td></tr>
<tr><td>ggsnMccMnc</td><td>String</td><td>O</td><td>It refers to a parameter that contains the Mobile Country Code (MCC) and Mobile Network Code (MNC) of the Gateway GPRS Support Node (GGSN) in a 3GPP (3rd Generation Partnership Project) network.
The data will be extracted from AVP '3GPP-GGSN-MCC-MNC' and populated from the last occurrence of the relevant information in the message.</td></tr>
<tr><td>preEmptionCapability</td><td>String</td><td>O</td><td>Defines whether a service data flow can get resources that were already assigned to another service data flow with a lower priority level.
The data will be extracted from AVP 'Pre-emption-Capability' and populated from the first occurrence of the relevant information in the message.
The mapped label value will be present in the xDRs.
<table>
<tr><th>Value</th><th>Mapped Label</th></tr>
<tr><td>0</td><td>Pre-emption Capability Enabled</td></tr>
<tr><td>1</td><td>Pre-emption Capability Disabled</td></tr>
</table></td></tr>
<tr><td>preEmptionVulnerability</td><td>String</td><td>O</td><td>Defines whether a service data flow can lose the resources assigned to it in order to admit a service data flow with higher priority level.
The data will be extracted from AVP 'Pre-emption-Vulnerability' and populated from the first occurrence of the relevant information in the message.
The mapped label value will be present in the xDRs.
<table>
<tr><th>Value</th><th>Mapped Label</th></tr>
<tr><td>0</td><td>Pre-emption Vulnerability Enabled</td></tr>
<tr><td>1</td><td>Pre-emption Vulnerability Disabled</td></tr>
</table></td></tr>
</table>

Table 3-4   Optional xDR Content

<table>
<tr><th>Field Name</th><th>Data Type</th><th>Presence</th><th>Description</th></tr>
<tr><td>pdnAddressV4</td><td>String</td><td>O</td><td>It indicates the IPv4 address(if available) of the access node gateway (SGW for 3GPP and AGW for non-3GPP networks) contained in Framed-IP-Address AVP.
The data will be extracted from AVP 'Framed-IP-Address' and populated from the first occurrence of the relevant information in the message.</td></tr>
<tr><td>pdnAddressV6</td><td>String</td><td>O</td><td>It indicates the IPv6 address(if available) of the access node gateway (SGW for 3GPP and AGW for non-3GPP networks) contained in Framed-IPv6-Prefix AVP.
The data will be extracted from AVP 'Framed-IPv6-Prefix' and populated from the first occurrence of the relevant information in the message.</td></tr>
<tr><td>apn</td><td>String</td><td>O</td><td>It indicates the PDN connection to which specific information refers e.g. APN.
The data will be extracted from AVP 'Called-Station-Id' and populated from the first occurrence of the relevant information in the message.</td></tr>
<tr><td>nodeType</td><td>String</td><td>O</td><td>Type of Node (Rule, Bearer, Session, Transaction).
The data will be extracted from AVP 'Node-Type' and populated from the first occurrence of the relevant information in the message.
The mapped label value will be present in the xDRs.
<table>
<tr><th>Value</th><th>Mapped Label</th></tr>
<tr><td>0</td><td>Rule</td></tr>
<tr><td>1</td><td>Bearer</td></tr>
<tr><td>2</td><td>Transaction</td></tr>
<tr><td>3</td><td>SubSession</td></tr>
<tr><td>4</td><td>Session</td></tr>
</table></td></tr>
</table>

Note

In case of SUDR, if xDR attributes' values are present in the inbound message, they will be added in the xDR records.

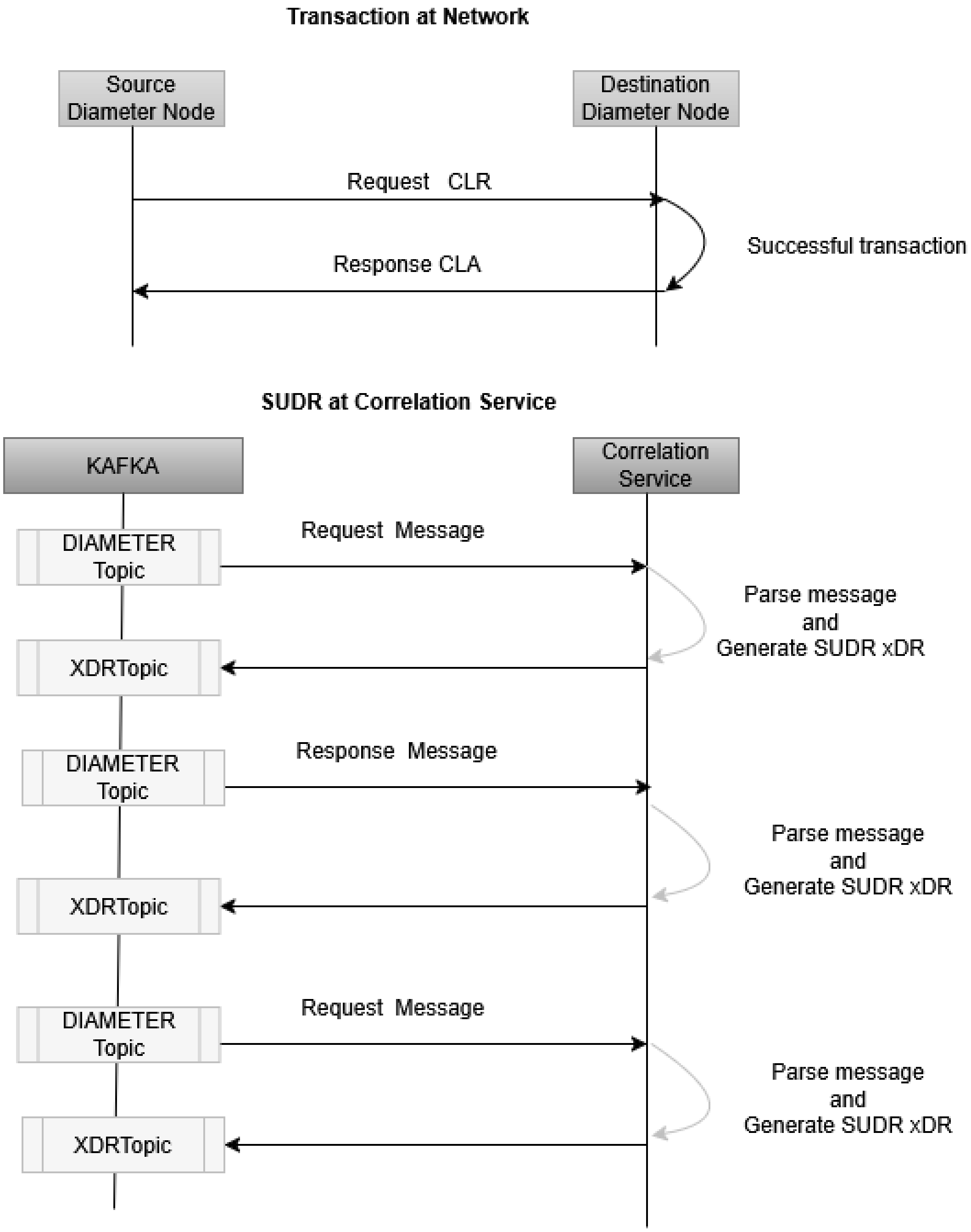
3.2.12.1.6 Correlation Mode

This section provides the details of the correlation modes supported by OCNADD.

SUDR xDR

OCNADD generates an SUDR type xDR for each message.

Figure 3-11   SUDR xDR



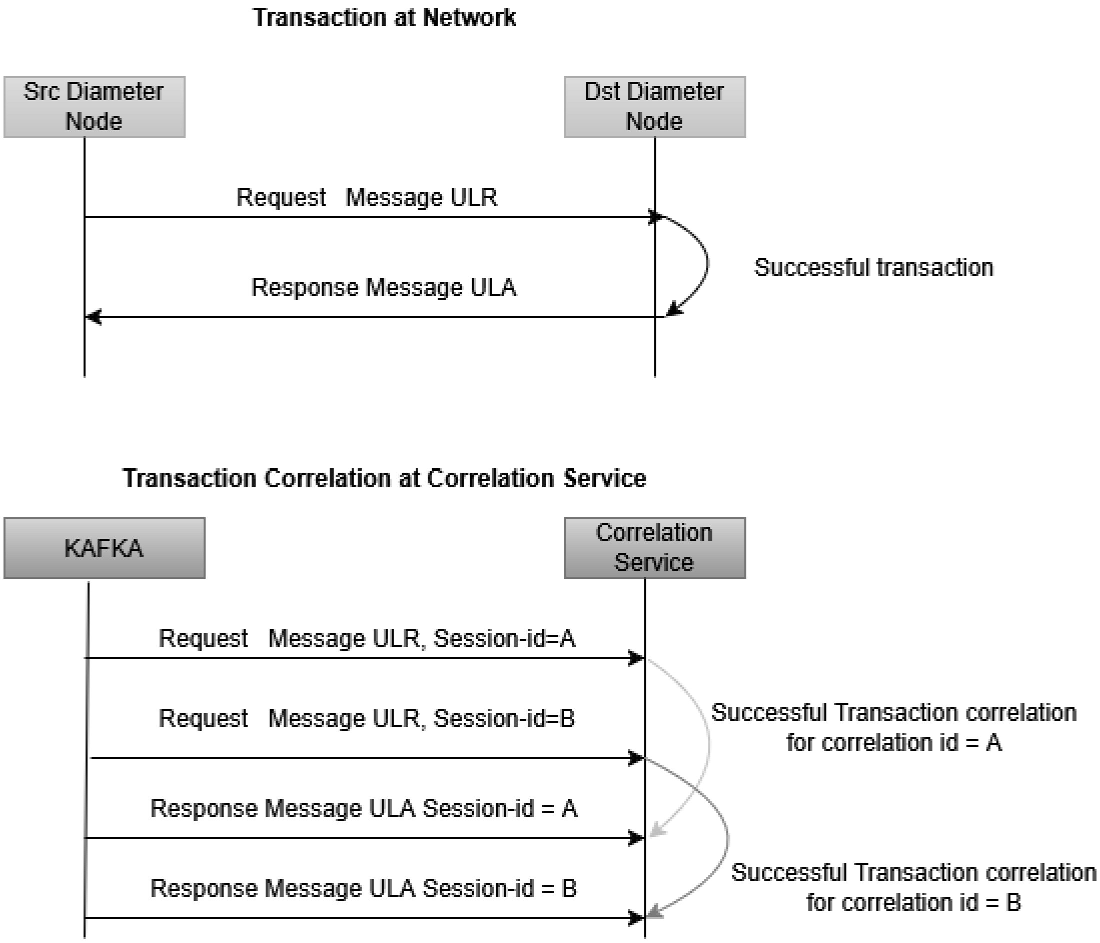
TRANSACTION XDR

> **Note**
>
> **Note:**
>
> - When messages received in Data Director (DD) are not in order, transaction correlation may be impacted, and correlation will be performed as per the order in which messages are received in DD.
> - In case of an upgrade, service restart, or re-balancing, some duplicate xDRs with correlation impact may get written into the xDR topic.
> - End-to-end latency of the Diameter feed is not applicable for Correlation Feed. End-to-end latency of TDR will be based on the completion of transactions.

Complete Transaction

When both the request message and response message have been received, a successful transaction xDR is generated with xDR status = Complete.

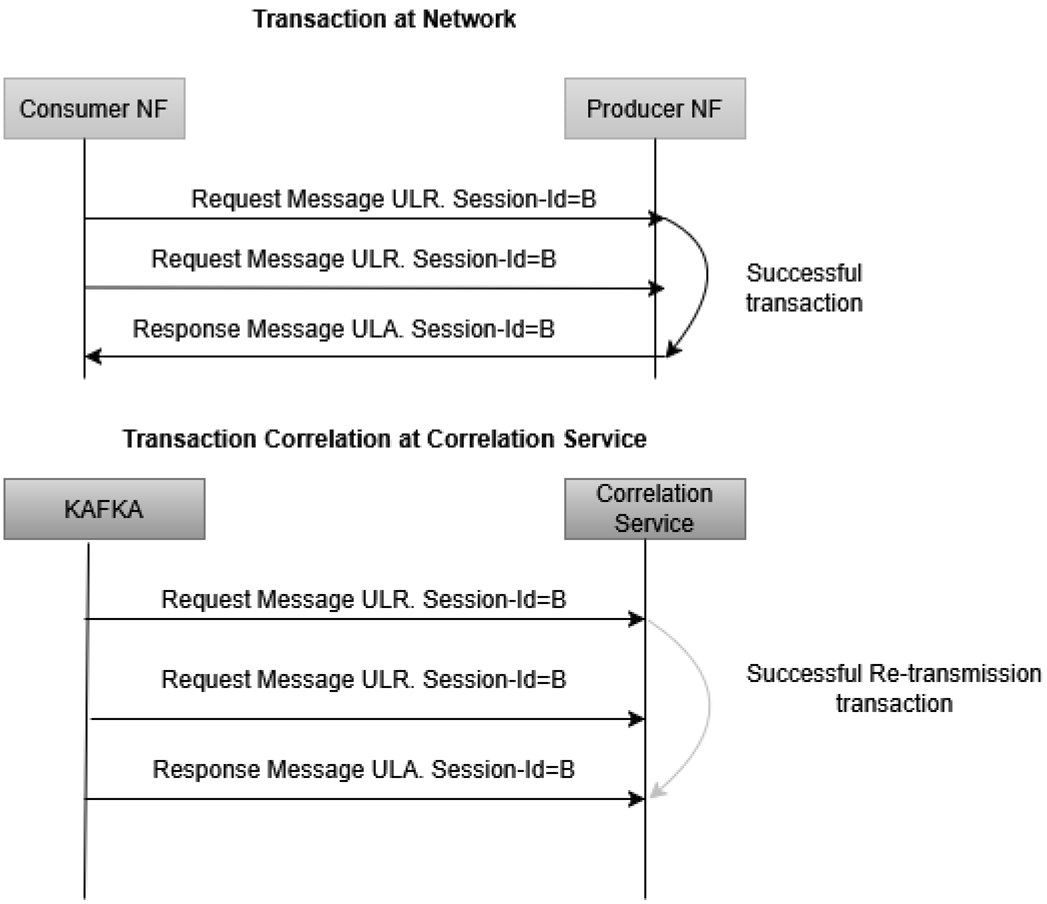
Figure 3-12 Complete Transaction


Transaction at Network
Src Diameter Node
Dst Diameter Node
Request Message ULR
Response Message ULA
Successful transaction
Transaction Correlation at Correlation Service
KAFKA
Correlation Service
Request Message ULR, Session-id=A
Request Message ULR, Session-id=B
Response Message ULA Session-id = A
Response Message ULA Session-id = B
Successful Transaction correlation for correlation id = A
Successful Transaction correlation for correlation id = B

Complete Re-transmission Transaction

When a request message is resent or re-transmitted within the duration of a transaction, it is referred to as re-transmission.

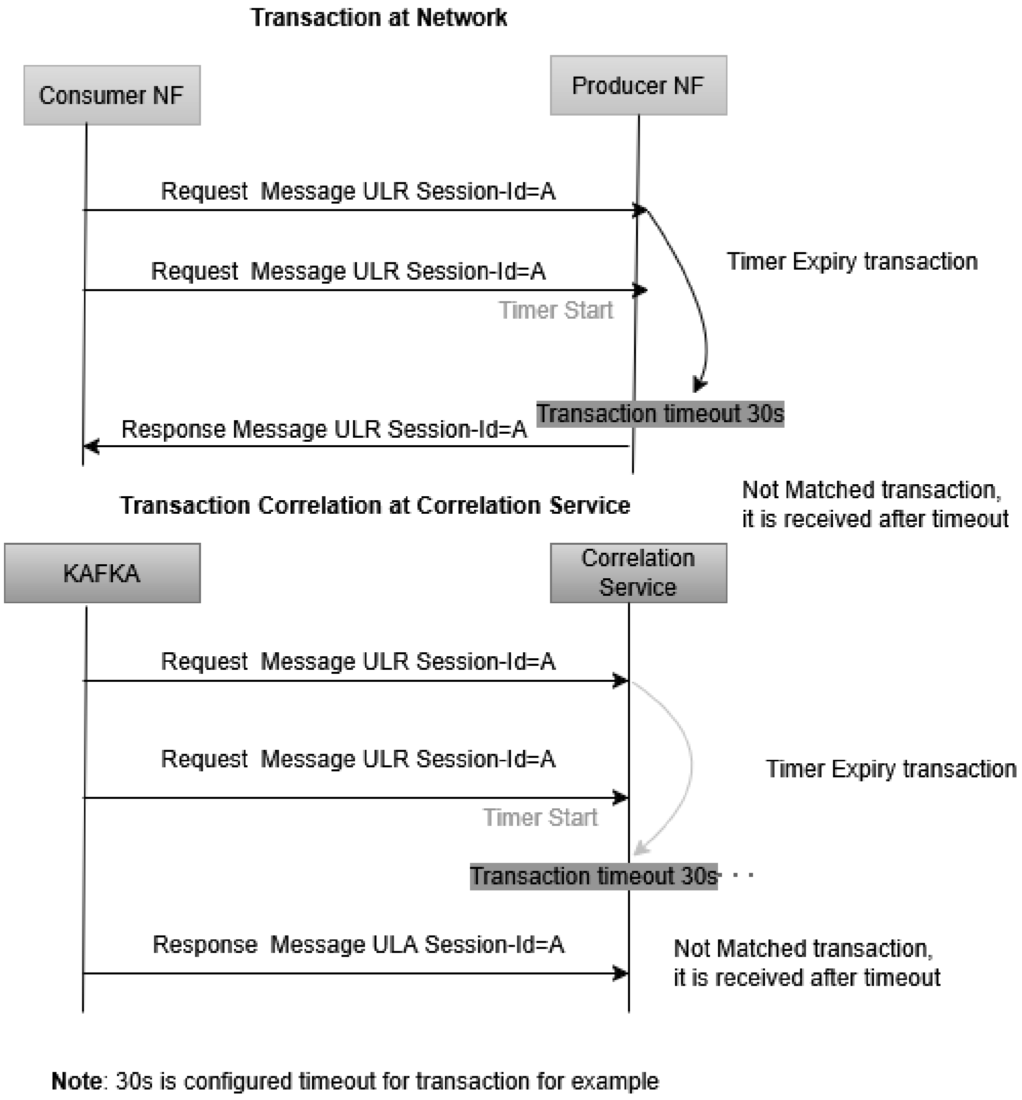
Figure 3-13 Complete Re-transmission Transaction


Transaction at Network
Consumer NF
Producer NF
Request Message ULR. Session-Id=B
Request Message ULR. Session-Id=B
Response Message ULA. Session-Id=B
Successful transaction
Transaction Correlation at Correlation Service
KAFKA
Correlation Service
Request Message ULR. Session-Id=B
Request Message ULR. Session-Id=B
Response Message ULA. Session-Id=B
Successful Re-transmission transaction

Timer Expiry Transaction

When the request message has only been received and the response message has either not been received or received after transaction duration, Timer expiry xDR is generated with xDR status = TimerExpiry.

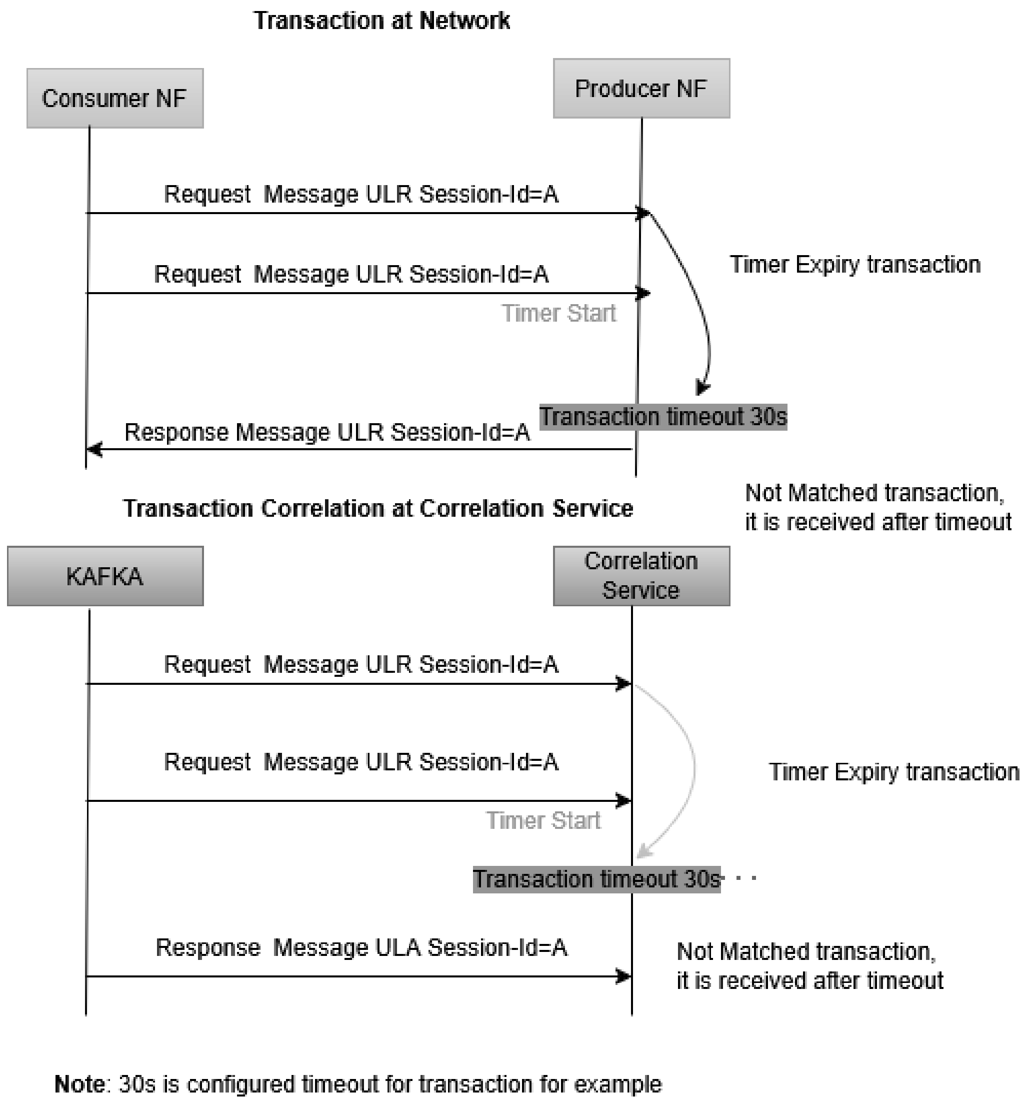
Figure 3-14 Timer Expiry Transaction


Transaction at Network
Consumer NF
Producer NF
Request Message ULR Session-Id=A
Request Message ULR Session-Id=A
Timer Start
Timer Expiry transaction
Transaction timeout 30s
Response Message ULR Session-Id=A
Not Matched transaction,
it is received after timeout
Transaction Correlation at Correlation Service
KAFKA
Correlation Service
Request Message ULR Session-Id=A
Request Message ULR Session-Id=A
Timer Start
Timer Expiry transaction
Transaction timeout 30s
Response Message ULA Session-Id=A
Not Matched transaction,
it is received after timeout
Note: 30s is configured timeout for transaction for example

Timer Expiry Re-transmission Transaction

When a request message has not been received with multiple retries but response message has either not been received or received after transaction duration, Timer expiry xDR is generated with xDR status = TimerExpiry.

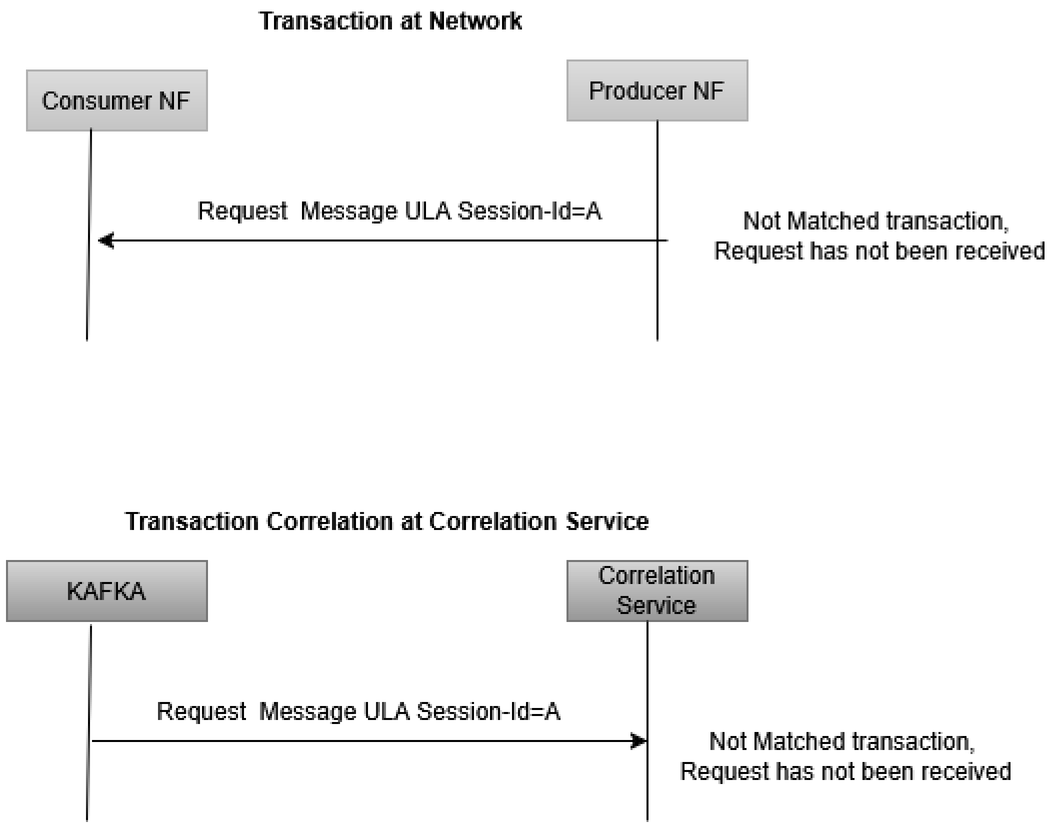
Figure 3-15 Timer Expiry Re-transmission Transaction


Transaction at Network
Consumer NF
Producer NF
Request Message ULR Session-Id=A
Request Message ULR Session-Id=A
Timer Start
Timer Expiry transaction
Transaction timeout 30s
Response Message ULR Session-Id=A
Not Matched transaction,
it is received after timeout
Transaction Correlation at Correlation Service
KAFKA
Correlation Service
Request Message ULR Session-Id=A
Request Message ULR Session-Id=A
Timer Start
Timer Expiry transaction
Transaction timeout 30s
Response Message ULA Session-Id=A
Not Matched transaction,
it is received after timeout
Note: 30s is configured timeout for transaction for example

Not Matched Transaction

When a request message has not been received due to a network issue and only a response message has been received, Not Matched xDR is generated with xDR status = Not Matched.

Figure 3-16 Not Matched Transaction


Transaction at Network
Consumer NF
Producer NF
Request Message ULA Session-Id=A
Not Matched transaction,
Request has not been received
Transaction Correlation at Correlation Service
KAFKA
Correlation Service
Request Message ULA Session-Id=A
Not Matched transaction,
Request has not been received

3.2.12.1.7 Correlation KPIs

These KPIs can be configured with correlation configuration. The selected KPIs in correlation configuration can be visualized in DD UI through the KPI dashboard.

Table 3-5 Supported KPIs

Metric Type	Details
TOTAL_TRANSACTION	Metrics Name: `ocnadd_total_transactions` Tag: app, mediationGroup, relayAgent, protocol, xdrStatus
TOTAL_SUCCESSFUL_TRANSACTION_PER_RESULT_CODE	Metrics Name: `ocnadd_total_transactions` Tag: app, resultCode, status, mediationGroup, relayAgent, xdrStatus, protocol
TOTAL_SUCCESSFUL_TRANSACTION_PER_APPLICATION_ID	Metrics Name: `ocnadd_total_transactions` Tag: app, applicationId, status, mediationGroup, relayAgent, xdrStatus, protocol
TOTAL_SUCCESSFUL_TRANSACTION	Metrics Name: `ocnadd_total_transactions` Tag: app, status, mediationGroup, relayAgent, xdrStatus, protocol
TOTAL_FAILED_TRANSACTION_PER_RESULT_CODE	Metrics Name: `ocnadd_total_transactions` Tag: app, resultCode, status, mediationGroup, relayAgent, xdrStatus, protocol

Table 3-5 (Cont.) Supported KPIs

Metric Type	Details
TOTAL_FAILED_TRANSACTION_PER_APPLICATION_ID	Metrics Name: `ocnadd_total_transactions` Tag: app, applicationId, status, mediationGroup, relayAgent, xdrStatus, protocol
TOTAL_FAILED_TRANSACTION	Metrics Name: `ocnadd_total_transactions` Tag: app, status, mediationGroup, relayAgent, xdrStatus, protocol
DIAMETER_TRANSACTION_LATENCY_PER_APPLICATION_ID	Metrics Name: `ocnadd_diameter_transcation_latency` Tag: app, resultCode, applicationId, status, mediationGroup, relayAgent, xdrStatus, protocol, sessionId, transactionTime **Note**: Enable for debugging only for a short duration. Metrics will be pegged only for those transactions whose latency is more than the helm-configured latency threshold value (default: 5s).

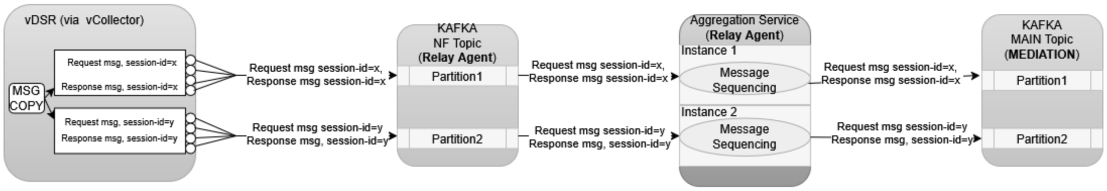
3.2.13 Message Sequencing

This feature enables message sequence delivery for messages of a Diameter transaction from Data Director (DD) to a third-party application.

Note:

- Key/custom based message writing from vCollector must be enabled.
- It is recommended to use RF > 1 for Kafka topics to avoid data loss in case of broker or topic partition failure.
- In the case of an upgrade, rollback, or service restart, duplicate messages will be sent by the aggregation service to avoid data loss, and message sequencing will be impacted during that time.

Figure 3-17 Diameter Message Sequencing


vDSR (via vCollector)
MSG COPY
Request msg, session-id=x
Response msg, session-id=x
Request msg, session-id=y
Response msg, session-id=y
Request msg session-id=x,
Response msg session-id=x
Request msg session-id=y
Response msg, session-id=y
KAFKA
NF Topic
(Relay Agent)
Partition1
Partition2
Request msg session-id=x,
Response msg session-id=x
Request msg session-id=y
Response msg, session-id=y
Aggregation Service
(Relay Agent)
Instance 1
Message Sequencing
Instance 2
Message Sequencing
Request msg session-id=x,
Response msg session-id=x
Request msg session-id=y
Response msg, session-id=y
KAFKA
MAIN Topic
(MEDIATION)
Partition1
Partition2

There are 2 modes to do message sequencing:

1. Time Based Message Sequencing (Windowing)
2. Transaction Based Message Sequencing

Helm Parameters

Table 3-6 Helm Parameters

Parameter	Description	Value
MESSAGE_SEQUENCING_TYPE	• Defines the type of message sequencing. • The default value is **NONE**, which means no message sequencing. • When any message sequencing is enabled, the end-to-end latency time shall increase based on the configured time corresponding to the message sequencing mode. • Only one message sequencing mode can be enabled at a time. • The parameter can be configured separately in the relay agent's Helm chart for each Diameter aggregation service. • **When any wrong or unsupported value is passed in MESSAGE_SEQUENCING_TYPE, it will fall back to the default option (NONE).**	• NONE • TIME_WINDOW • TRANSACTION
WINDOW_MSG_SEQUENCING_EXPIRY_TIMER	• This parameter defines the time for window-based message sequencing and it is present in the mediation Helm chart. • This must be set when **MESSAGE_SEQUENCING_TYPE = TIME_WINDOW.** • **When any wrong or unsupported value is passed, it will fall back to the default (10 ms).**	Range: 5ms-500ms Default: 10ms
TRANSACTION_MSG_SEQUENCING_EXPIRY_TIMER	• This parameter defines the time for transaction-based message sequencing and it is present in the mediation Helm chart. • This must be set when **MESSAGE_SEQUENCING_TYPE = TRANSACTION.** • **When any wrong or unsupported value is passed, it will fall back to the default (200 ms).**	Range: 20ms-60s Default: 200ms
MESSAGE_REORDERING_INCOMPLETE_TRANSACTION_METRICS_ENABLE	• This parameter can be enabled in the mediation Helm chart when the requirement is to check metrics for failure of message reordering or incomplete transactions. • Metrics Name: `ocnadd_message_reordering_incomplete_transaction_count` • The metrics will be pegged for MESSAGE_SEQUENCING_TYPE = REQUEST_RESPONSE or TRANSACTION.	Range: true/false Default: false

1. **Time-Based Message Sequencing (Windowing)**
   This mode enables re-ordering of unordered messages based on the timestamp present in the message. The group of messages received within the window time for each partition separately will be considered for message sequencing.

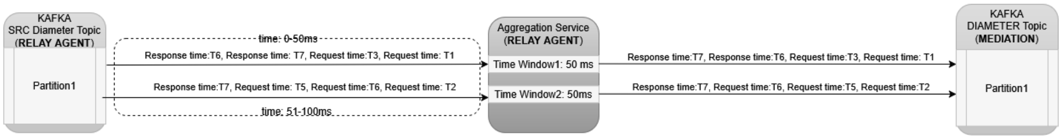
   For each partition, when time-based sequencing is completed, all the sequenced messages will stream to the mediation's Kafka DIAMETER topic.

   Helm Parameters:

   - MESSAGE_SEQUENCING_TYPE: TIME_WINDOW
   - WINDOW_MSG_SEQUENCING_EXPIRY_TIMER: 10(ms), range: [5ms-500ms]

   > **Note**
   >
   > - This will add or increase the end-to-end message latency to the configured value of `WINDOW_MSG_SEQUENCING_EXPIRY_TIMER` and the processing time.
   > - Older timestamp messages from a different window can be seen in the partition, as multiple threads will be writing data into the same partition in parallel (source topic partition count < target topic partition count). The aim is to achieve transaction sequencing.

   Figure 3-18 Time Based Message Sequencing


KAFKA
SRC Diameter Topic
(RELAY AGENT)
Partition1
time: 0-50ms
Response time:T6, Response time: T7, Request time:T3, Request time: T1
Response time:T7, Request time: T5, Request time:T6, Request time: T2
time: 51-100ms
Aggregation Service
(RELAY AGENT)
Time Window1: 50 ms
Time Window2: 50ms
Response time:T7, Response time:T6, Request time:T3, Request time: T1
Response time:T7, Request time:T6, Request time:T5, Request time:T2
KAFKA
DIAMETER Topic
(MEDIATION)
Partition1

2. **Transaction Based Message Sequencing**
   This mode enables re-ordering of unordered messages based on the transaction (RxRequest, TxRequest, RxResponse, TxResponse).

   Sequencing Rule:

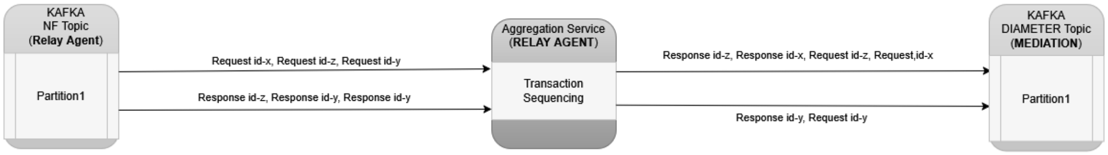
   - **Transaction order:** Request, Response
   - When all messages of a transaction (RxRequest, TxRequest, RxResponse, TxResponse) are received in order, the message will be streamed to the mediation's Kafka DIAMETER topic without any delay.
   - When TxRequest is received before RxRequest for a transaction, it will be sent in order when RxRequest is received or after `TRANSACTION_EXPIRY_TIME` expires.
   - When RxRequest and TxRequest are received in order and TxResponse is received before RxResponse, the RxRequest and TxRequest will be sent without any delay, and TxResponse shall be sent in order when RxResponse is received or after `TRANSACTION_EXPIRY_TIME` expires.
   - When RxResponse is received first, it will be sent when RxRequest and TxRequest are received or after `TRANSACTION_EXPIRY_TIME` expires.
   - When TxResponse is received first, it will be sent when RxRequest, TxRequest, and TxResponse are received or after `TRANSACTION_EXPIRY_TIME` expires.

   Helm Parameters:

- `MESSAGE_SEQUENCING_TYPE`: TRANSACTION
- `TRANSACTION_MSG_SEQUENCING_EXPIRY_TIMER`: 200 ms, range: [20 ms – 120 s]

> **Note**
>
> This will add or increase the end-to-end message latency up to the configured value of `TRANSACTION_MSG_SEQUENCING_EXPIRY_TIMER` and the processing time.

Figure 3-19 Transaction Based Message Sequencing


KAFKA
NF Topic
(Relay Agent)
Partition1
Request id-x, Request id-z, Request id-y
Response id-z, Response id-y, Response id-y
Aggregation Service
(RELAY AGENT)
Transaction
Sequencing
Response id-z, Response id-x, Request id-z, Request,id-x
Response id-y, Request id-y
KAFKA
DIAMETER Topic
(MEDIATION)
Partition1

4 User Interface

The current release does not support Diameter configuration and visualization through the UI.

5

Parameter Update in OCNADD Microservices

This section describes the procedure to update the parameters and container images of the various OCNADD services for Diameter feed.

> ⓘ **Note**
>
> In case of an upgrade, rollback, service restart, or if a configuration is created with the same name, duplicate xDRs will be generated by the correlation service to avoid data loss.

For updates and details on parameters of the Relay Agent, Mediation Group, and Management Group services, see "Parameter Update in OCNADD Microservices" section in the *Oracle Communications Network Analytics Data Director User Guide*.

6

Kafka & Communication Management

This chapter outlines the administrative, security, and operational procedures required to manage Kafka infrastructure and external communication within OCNADD, ensuring reliable data flow, controlled access, and secure service interactions.

6.1 Kafka Cluster Management Procedures

This section outlines the operational steps required to maintain Kafka clusters used by OCNADD.

To perform the following operations, see "Kafka Cluster Management Procedures" section in the *Oracle Communications Network Analytics Data Director User Guide*.

- Kafka topic creation
- Kafka cluster capacity expansion
  - Adding a broker to an existing Kafka cluster
  - Adding a partition to an existing topic
  - Partition reassignment in Kafka cluster
- Kafka cluster external access
  - External access with OCCNE LBVM
  - External access with OCCNE CNLB
- Enabling Kafka log retention policy
- Expanding Kafka storage
- Enabling RAM storage in Kafka cluster
- Disabling RAM storage in Kafka cluster

> **Note**
>
> For each worker group, source topics (inbound Diameter data from Diameter applications to the Data Director), such as vcollector, dsr, and pcf, are created and managed in the Relay Agent’s Kafka cluster. In contrast, destination topics (outbound Diameter data from the Data Director to third-party applications), such as diameter and <xdr>-correlated, are created and managed in the Mediation Group’s Kafka cluster.

6.2 Enable External Communication Between OCNADD Gateways

Prerequisites

- mTLS should be enabled

- External IPs must be used to create the certificates. There will not be any dynamic IP addresses for gateway external communication; users need to provide static IPs and configure the certificates with these IPs.

To perform the following operations, see "Enable External Communication Between OCNADD Gateways" section in the *Oracle Communications Network Analytics Data Director User Guide*.

- OCNADD Gateway External Access in OCCNE LBVM
- OCNADD Management Gateway External Access
- OCNADD Mediation Gateway External Access
- OCNADD Relay Agent Gateway External Access
- OCNADD Gateway External Access in OCCNE CNLB

6.3 Update Certificate of The Existing Services

To update OCNADD service certificates, see "Update Certificate of the Existing Services" section in the *Oracle Communications Network Analytics Data Director User Guide*.

6.4 Enable Kafka Feed Configuration Support

This section lists the prerequisites for the Diameter Node or vCollector to communicate with the Data Director Relay Agent Kafka cluster, and for third-party consumer applications to communicate with the Data Director Mediation Kafka cluster securely. The section also lists the configuration settings that need to be done on the Kafka broker.

There are certain preconditions that must be met before the Kafka feed for external consumer applications can work correctly. Some of these settings may disrupt communication with producer clients, especially if any client ACL rule is configured in Kafka. In that case, Kafka will authenticate and authorize each and every client, and existing clients will be disrupted if they are not already using SASL_SSL or SSL (mTLS) connections and recommendations from the Oracle Communications Network Analytics Data Director Security Guide.

> **Note**
>
> The procedure mentioned below should be executed on the corresponding Relay Agent and Mediation Group on which the Kafka feed configuration support is being enabled.

To perform the following operations, see "Enable Kafka Feed Configuration Support" section in the *Oracle Communications Network Analytics Data Director User Guide*.

- Prerequisites for Diameter producer (The steps for NF Producer also apply to Diameter producers like vCollector and DSR, etc.)
- Prerequisites for External Consumers
- Update OCNADD Configuration
- Update JAAS Configuration with Users
- Update SCRAM Configuration with Users
- Create Client ACLs
- Delete Generic Producer Client ACLs

6.5 Disable Kafka Feed Configuration Support

The section defines the procedure that should be executed when external Kafka feeds are no longer used in the Data Director deployment.

External Kafka feeds require TLS and access control in the Kafka server; if external Kafka feed support is not required, then access control in Kafka can be disabled.

The steps in this procedure should only be executed on the Mediation Group in which Kafka feed support is required to be disabled.

> **Note**
>
> - In the case of a rollback to a release where Kafka feed support was not present, it is mandatory to delete the producer client ACLs and Kafka feeds before the rollback is initiated. Follow steps 1 and 3 for deleting the feeds and ACLs.
> - In the case of a rollback to a revision where Kafka feeds were supported and configured, there is no need to delete Kafka feeds and producer client ACLs.
> - If it is not possible to delete the ACLs and feeds before the rollback, contact Oracle Support using MOS.

To disable Kafka Feed, see the steps mentioned in the section "Disable Kafka Feed Configuration Support" section in the *Oracle Communications Network Analytics Data Director User Guide*.

6.6 Configuring "Host" based ACLs for Kafka Feed

The Kafka Feed supports optional "host"-based ACLs for the external consumer application. This allows an external application to connect from a specific client machine with a specific IP address. The client application can be running inside a pod in a Kubernetes cluster where OCNADD is deployed, or in a different cluster. Since pods do not have static IP addresses, "host"-based ACLs are optional for Kafka feeds. The client machine hosting the external Kafka application can also be a separate virtual machine in the customer cloud environment; in this case, a static IP address can be given to the client VM running the external Kafka consumer application.

The Kafka Feed configuration has a "hostname" field, which is optional and currently supports only a single IP address. The default behavior of the Kafka feed is to allow all hosts. This default behavior applies when the user leaves the Host Name field blank or provides the wildcard character *.

The Host Name field can be either of the following:

- IPv4 address of the host where the consumer application is running
- Blank or wildcard character * (this allows all host IPs)

Note

- Pod/VM hostname-based ACLs are not yet supported in Kafka
- IPv6 is not supported
- A specific host IP ACL is recommended when a static IP is used for the client machine
- The host IP should not be configured for cloud-native client applications running in a K8s cluster, since pods have dynamic IP assignment

To perform the following operations, see "Configuring 'Host' based ACLs for Kafka Feed" section in the *Oracle Communications Network Analytics Data Director User Guide*.

- Adding network IP "Host" ACLs in Kafka Feed
- Deleting network IP "Host" ACLs in Kafka Feed

6.7 Enable/Disable Traffic Segregation Using CNLB in the Data Director

This section defines the procedure to enable or disable traffic segregation in the Data Director. The procedures are applicable only when CNLB is supported in OCCNE. The Data Director currently supports traffic segregation and external access using CNLB for the following:

- Kafka cluster external access using CNLB ingress NADs and external IPs

To perform the following operations, see "Enable/Disable Traffic Segregation Using CNLB in the Data Director" in the *Oracle Communications Network Analytics Data Director User Guide*.

- Enable traffic segregation in the Data Director
- Disable traffic segregation in the Data Director

7

Metrics, KPIs, Alerts, and Alarms

This chapter details the Metrics, KPIs, Alerts, and Alarms used by OCNADD.

7.1 Metrics, Dimensions, and Common Attributes

This section defines the metrics, dimensions, and attributes used by OCNADD.

7.1.1 Dimensions and Common Attributes

This section includes information about Dimensions and Common Attributes of metrics for OCNADD.

Dimensions

The following table includes information about dimensions of OCNADD.

Table 7-1 Dimensions

Dimension	Values / Type	Description
quantile	Integer values	It captures the latency values with ranges: 10 ms, 20 ms, 40 ms, 80 ms, 100 ms, 200 ms, 500 ms, 1000 ms, and 5000 ms.
instance_identifier	Prefix configured in Helm, UNKNOWN	Prefix of the pod configured in Helm when there are multiple instances in the same deployment.
processor_node_id	–	Stream processor node ID in the aggregation service.
serviceId	serviceType-N	Identifier for the service instance used for registration with the health monitoring service.
serviceType	CONFIGURATION, ALARM, OCNADD-ADMIN, AGGREGATION-DIAMETER, CORRELATION-DIAMETER	The OCNADD service type.
service	ocnaddadminservice, ocnaddconfiguration, ocnaddhealthmonitoring, ocnadddiameteraggregation, ocnadddiamtercorrelation	The name of the Data Director microservice.
request_type	Diameter Correlation	Type of the data feed created using REST; this is used to identify if the xDR feed is for HTTP2 or Diameter.
nf_feed_type	VCOLLECTOR	The source NF for the feed or the name of the Diameter data provider.
correlation-id	–	Taken from the correlation-id present in the metadata list.

Table 7-1 (Cont.) Dimensions

Dimension	Values / Type	Description
way	–	Taken from the message-direction present in the metadata list.
srcIP	–	Obtained from the source IP address present in the metadata list of the Diameter message sent by vCollector.
dstIP	–	Obtained from the destination IP address present in the metadata list of the Diameter message sent by vCollector.
srcPort	–	Obtained from the source port present in the metadata list of the Diameter message sent by vCollector.
dstPort	–	Obtained from the destination port present in the metadata list of the Diameter message sent by vCollector.
worker_group	String	Name of the worker group in which the corresponding traffic processing services (relay agent and mediation groups) are running.
relay_agent_group	String	The name of the relay agent group through which the Diameter message from vCollector is transmitted and where processing services are running.
mediation_group	String	The name of the mediation group where xDR processing services are running, allowing third-party applications to consume the processed data.

Attributes

The following table includes information about common attributes of OCNADD.

Table 7-2 Attributes

Attribute	Description
application	The name of the application that the microservice is a part of.
microservice	The name of the microservice.
namespace	The Kubernetes namespace in which the microservice is running.
node	The name of the worker node that the microservice is running on.
pod	The name of the Kubernetes pod.

7.1.2 Metrics

This section provides information about important metrics related to OCNADD.

To retrieve the following Diameter metrics and other supported OCNADD metrics, see "OCNADD Metrics" section in the *Oracle Communications Network Analytics Data Director User Guide*.

- `kafka_stream_processor_node_process_total`
- `kafka_stream_processor_node_process_rate`
- `kafka_stream_task_dropped_records_total`
- `kafka_stream_task_dropped_records_rate`
- `ocnadd_health_total_alarm_raised_total`
- `ocnadd_health_total_alarm_cleared_total`
- `ocnadd_health_total_active_number_of_alarm_raised_total`
- `ocnadd_ext_kafka_feed_record_total`

7.2 KPIs

This section provides information about important KPIs related to OCNADD.

> **Note**
>
> - The **namespace** in the KPIs should be updated to reflect the current namespace used in the Data Director deployment.
> - The queries should be used per relay agent and/or mediation group of the worker group wherever applicable, such as KPIs for ingress and egress MPS, failure/success rate, packet drop, etc. The label **"worker_group"** should be used to filter based on the worker group name in the KPI queries.
> - The queries are in **PromQL** and **MQL** syntax. Use PromQL for CNE and MQL for OCI-based deployments.

To retrieve the following Diameter KPIs and other supported OCNADD KPIs, see "OCNADD KPIs" section in the *Oracle Communications Network Analytics Data Director User Guide*.

- `ocnadd_ingress_record_count_by_service`
- `ocnadd_ingress_record_count_total`
- `ocnadd_ingress_mps_per_service_10mAgg`
- `ocnadd_ingress_mps_10mAgg`
- `ocnadd_ingress_mps_per_service_10mAgg_last_24h`
- `ocnadd_ingress_record_count_per_service_10mAgg_last_24h`
- `ocnadd_kafka_ingress_record_drop_rate_10minAgg`
- `ocnadd_kafka_ingress_record_drop_rate_per_service_10minAgg`
- `ocnadd_ext_kafka_feed_record_total` per external feed rate (MPS)
- Memory Usage per POD
- CPU Usage per POD
- Service Status

7.3 Alerts

This section provides information about the OCNADD alerts and their descriptions

Alerts Interpretation

The table below defines the alert severity interpretation based on the infrastructure.

Table 7-3 Alerts Interpretation

Alert Severity	Interpretation
Critical	Critical
Major	Error
Minor	Error
Warning	Warning
Info	Info

> **Note**
>
> Alert OIDs are deprecated for OCI deployments.

For information on monitoring the following Diameter alerts and other supported OCNADD alerts, see "OCNADD Alerts" section in the *Oracle Communications Network Analytics Data Director User Guide*.

- System Level Alerts
- Application Level Alerts
- OCNADD Alert Configuration
- OCNADD configuration when Prometheus is deployed without operator

7.3.1 Adding SNMP Support

OCNADD forwards the Prometheus alerts as Simple Network Management Protocol (SNMP) traps to the southbound SNMP servers. OCNADD uses two SNMP MIB files to generate the traps. The alert manager configuration is modified by updating the `alertmanager.yaml` file. In the `alertmanager.yaml` file, the alerts can be grouped based on pod name, alert name, severity, namespace, and so on. The Prometheus alert manager is integrated with the Oracle Communications Cloud Native Core, Cloud Native Environment (CNE) **snmp-notifier** service. The external SNMP servers are set up to receive the Prometheus alerts as SNMP traps. The operator must update the MIB files along with the alert manager file to fetch the SNMP traps in their environment.

> **Note**
>
> - SNMP is not supported on OCI.
> - The following procedure requires admin privileges.

Procedures:

- Alert Manager Configuration
- Integrating with snmp-notifier service
- Verifying SNMP notification
- OCNADD MIB FILES

To configure the alert manager, see "Alert Manager Configuration" section in the *Oracle Communications Network Analytics Data Director User Guide*.

7.4 Alarms

This section provides information on all the alarms generated by OCNADD.

Alarm Types

The following table depicts the OCNADD alarm types and their ranges:

Table 7-4 Alarm Types

Alarm Type	Description	Range
SECURITY	Security Violation	1000–1999
COMMUNICATION	Communication Failure	2000–2999
QOS	Quality Of Service	3000–3999
PROCESSING_ERROR	Processing Error	4000–4999
OPERATIONAL_ALARMS	Operational Alarms	5000–5999

> ⓘ **Note**
>
> **Alarm Purge or Clear Criteria**
> The raised alarm will persist in the database and will be cleared or purged when either of the following conditions is met:
>
> - The corresponding service sends a clear alarm request to the Alarm service.
>   It is purged after the expiry of the configured purge alarm timeout. By default, it is **7 days**.

For information on using the following, see "OCNADD Alarms" section in the *Oracle Communications Network Analytics Data Director User Guide*:

- OCNADD OIDs
- Alarm Type
- Communication Failure Alarms
- Processing Error Alarms
- Operational Alarms