Oracle® Communications

Networks Data Analytics Function User Guide

Release 24.2.2
F96721-05
April 2025

Oracle Communications Networks Data Analytics Function User Guide, Release 24.2.2

F96721-05

Contents

10 OCNWDAF Alerts

My Oracle Support

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

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

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

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

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

Acronyms

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

Table Acronyms

Acronym	Description
3GPP	3rd Generation Partnership Project
5GC	5G Core Network
5GS	5G System
AF	Application Function
API	Application Programming Interface
AMF	Access and Mobility Management Function
AnLF	Analytics Logical Function
ASM	Aspen Service Mesh
CAP4C	Converged Analytics Platform for Communication
CNC	Cloud Native Core
CNE	Oracle Communications Cloud Native Core, Cloud Native Environment
CSP	Communications Service Provider
FE	Front End
FQDN	Fully Qualified Domain Name
GUI	Graphical User Interface
HTTPS	Hypertext Transfer Protocol Secure
KPI	Key Performance Indicator
HA	High Availability
IMSI	International Mobile Subscriber Identity
K8s	Kubernetes
MDT	Mobile Data Terminal
ME	Monitoring Events
MICO	Mobile Initiated Connection Only
ML	Machine Learning
MLOPs	Machine Learning Operations
MTLF	Model Training Logical Function
Network Slice	A logical network that provides specific network capabilities and network characteristics.
NEF	Oracle Communications Cloud Native Core, Network Exposure Function
NF	Network Function
NRF	Oracle Communications Cloud Native Core, Network Repository Function
NSI	Network Slice instance. A set of Network Function instances and the required resources (such as compute, storage and networking resources) which form a deployed Network Slice.
NSSF	Oracle Communications Cloud Native Core, Network Slice Selection Function

Table (Cont.) Acronyms

Acronym	Description
OCI	Oracle Cloud Infrastructure
OCNADD	Oracle Communications Network Analytics Data Director
OCNWDAF	Oracle Communications Networks Data Analytics Function
OAM	Operations, Administration, and Maintenance
PLMN	Public Land Mobile Network
RAN	Radio Access Network
REST	Representational State Transfer
SBA	Service Based Architecture
SBI	Service Based Interface
SMF	Session Management Function
SNMP	Simple Network Management Protocol
SUPI	Subscription Permanent Identifier
UDM	Unified Data Management
UE	User Equipment
UPF	User Plane Function
UDR	Oracle Communications Cloud Native Core, Unified Data Repository
UDM	Unified Data Management
URI	Uniform Resource Identifier

What's New in This Guide

This section introduces the documentation updates for Release 24.2.x in Oracle Communications Networks Data Analytics Function User Guide.

Release 24.2.2 - F96721-05, April 2025

Removed the **IPv6 Support** feature from the OCNWDAF Features section as NWDAF does not support IPv6.

Release 24.2.2 - F96721-04, November 2024

Added a new chapter, NWDAF Metrics.

Release 24.2.0 - F96721-02, September 2024

Updated the stem sentence of the 'Configure' section in Support for TLS 1.3 feature as "You can configure this feature using Helm parameters. Configure the following parameters in the Ingress Gateway and Egress Gateway, required for TLS1.3".

Release 24.2.0 - F96721-01, July 2024

- The following changes are made as part of the Deployment in OCI using OCI Adaptor feature:
  - Added the OCI acronym in the Acronyms section.
  - Added the *Oracle Communications Cloud Native Core, OCI Adaptor Deployment Guide* document in the References section.
- Added the following sections for the new features supported in this release:
  - Support for TLS 1.3
  - Support for Model C Communication
  - SNMP Support
- NF Load Analytics information is enhanced and the OCNADD can be configured as a data source for NF Load Analytics, the Network Function (NF) Load Analytics section is updated to include this information.
- Added the Dashboard and Alerts GUI screens.
- Added new section for OCNWDAF KPIs.

1 Introduction

The Oracle Communications Networks Data Analytics Function (OCNWDAF) is a Network Function (NF) that assists in collecting and analyzing data in a 5G network. This document provides information about the role of Oracle Communications Networks Data Analytics Function (OCNWDAF) in 5G Network Architecture and OCNWDAF services and managed objects.

1.1 Overview

Oracle Communications Network Data Analytics Function (OCNWDAF) is a Network Function (NF) in the 5G core network of the 5G network architecture.

About Oracle Communications Networks Data Analytics Function

The OCNWDAF enables the operator to collect and analyze the data in the network. The 5G technology requires prescriptive analytics to drive closed-loop automation and self-healing networks. In a 5G network, the term consumers include 5G NFs, Application Functions (AFs), and Operations, Administration, and Maintenance (OAM) and the data producers are NFs. The OCNWDAF supports the following functions:

- OCNWDAF collects data from Access and Mobility Management Function (AMF), Session Management Function (SMF), and Network Repository Function (NRF) in the network. OCNWDAF collects data directly from the NFs.
- The OCNWDAF is designed to provide analytics information to consumers such as NFs, AFs, and OAM.
- The OCNWDAF collects data from call flows across the 5G control plane through messages captured and filtered by the Oracle Communications Network Analytics Data Director (OCNADD).

A 5G network contains a vast number of devices and sensors generating an enormous amount of data. The OCNWDAF function allows the Communications Service Providers (CSPs) to efficiently monitor, manage, automate, and optimize their network operations by the analytics generated using the data collected across the network. The OCNWDAF also helps the CSPs in achieving the operational efficiency and provides an enhanced service experience.

The analytics information provided by the OCNWDAF is either statistical information based on past events or predictive information. The consumers can subscribe or unsubscribe for specific analytics information as a one-time event or periodically get notified when a specifically defined event (for example, a threshold is breached) is detected. The analytics information provides insights to balance the resources on the network.

An OCNWDAF consumer can avail analytics information for different analytic events. The OCNWDAF can predict the User Equipment (UE) location and also detect if the UE is in an abnormal location. Based on the analytics information, the CSPs can roll out new services or modify the existing services without waiting for a maintenance window in the network. This ensures lesser chances of the network experiencing downtime.

The NRF discovers the OCNWDAF instances for the NF consumers in the network. The OCNWDAF information can also be locally configured on the NF consumers. The OCNWDAF selection function in the consumer NF selects an OCNWDAF instance among available

OCNWDAF instances. Different OCNWDAF instances present in the 5G network can be configured to provide a specific type of analytics information. This information about the OCNWDAF instance is described in the OCNWDAF profile stored in the NRF. The consumer NFs that need specific analytics information, query the NRF with the required Analytics ID.

OCNWDAF installation is supported over the following platforms:

- Oracle Communications Cloud Native Core, Cloud Native Environment (CNE)
- Oracle Cloud Infrastructure (OCI)
  For more information, see *Oracle Communications Networks Data Analytics Function Installation, Upgrade, and Fault Recovery Guide*.

> **Note**
>
> The performance and capacity of the OCNWDAF system may vary based on the call model, Feature / Interface configuration, and underlying CNE and hardware environment.

1.2 References

For more information about OCNWDAF, refer to the following documents:

- *Oracle Communications Networks Data Analytics Function Solution Guide*
- *Oracle Communications Networks Data Analytics Function Installation, Upgrade, and Fault Recovery Guide*
- *Oracle Communications Networks Data Analytics Function Troubleshooting Guide*
- *Oracle Communications Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide*
- *3GPP Technical Specification 29.520, 5G System Network Data Analytics Services*
- *3GPP Technical Specification 23.288, Architecture enhancements for 5G System (5GS) to support Network Data Analytics Services*
- *3GPP Technical Specification 29.508, 5G System Session Management Event Exposure Services*
- *3GPP Technical Specification 29.510, 5G System Network Function Repository Services*
- *3GPP Technical Specification 29.518, 5G System Access and Mobility Management Services*
- *Oracle Communications Cloud Native Core, OCI Adaptor Deployment Guide*

2
OCNWDAF Architecture

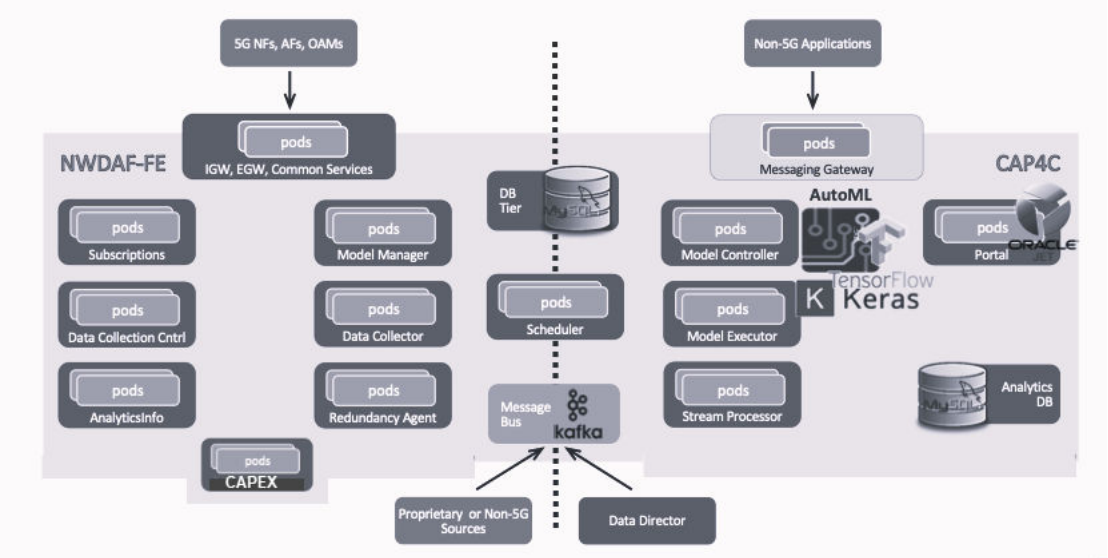
This chapter describes the OCNWDAFs detailed design and architecture.

2.1 Oracle Communications Networks Data Analytics Function Architecture

OCNWDAF comprises of various microservices deployed in a Kubernetes based Cloud Native Environment (for example, CNE). The environment has some common services for logs (or metrics) collection, analysis, graphs or charts visualization, and so on. The OCNWDAF uses standard interfaces from the Service Based Architecture (SBA) to collect data through subscription or request model from other Network Functions (NFs). The microservices integrate with the environment and provide the necessary data analytics.

The following diagram depicts the OCNWDAF architecture:

Figure 2-1 OCNWDAF Architecture



The OCNWDAF architecture aligns with 3GPP Release 17 Technical Specifications.

OCNWDAF Front End

The OCNWDAF Front End (FE) interacts with 5G NFs to gather information through the Service Based Architecture (SBA) or Service Based Interface (SBI) defined in 3GPP 23.288 and 29.520 Technical Specifications.

- Collects data from 5G NFs
- Provides the data to backend Converged Analytics Platform for Communication (CAP4C)

- Collects the processed analytics information from CAP4C
- Provides the analytics information to the consumer NFs and Application Functions (AFs)

Converged Analytics Platform for Communication (CAP4C)

The Analytics Engine, CAP4C is the core of the OCNWDAF, it supports data collection from the Front End (FE) module. Machine Learning (ML) models process the collected data. The Analytics Engine performs predictive or descriptive data analysis and provides analytics information through real-time stream processing.

- Processes data from the Front End (FE) or data received from the OCNADD
- Examines streaming data in real time to allow thresholding and other use cases
- Generates OCNWDAF analytics information (Statistical, Predictive, and Abnormal Behavior)
- Automates machine learning models
- Provides visualization and reports

Oracle Communications Network Analytics Data Director (OCNADD)

- Receives messages from Oracle NFs such as SCP, SEPP, and NRF.
- Captures the call flow messages transmitted between the control plane NFs.
- Filters data from the call flows and sends it to the CAP4C.

A few common services are deployed with the OCNWDAF. The common services are also used by other 5G NFs along with OCNWDAF.

Ingress Gateway

This microservice is an entry point for accessing OCNWDAF supported service operations and provides the functionality of an OAuth validator.

Egress Gateway

This microservice is responsible to route OCNWDAF initiated egress messages to other NFs.

For more information about Ingress and Egress Gateway, see *Oracle Communications Cloud Native Core, Cloud Native Environment User Guide*.

Scheduler

Offers scheduling services for timed events such as periodic consumer report notifications.

Model Manager

- Tracks the analytics requests, timeframes, and data items required within the training data set to train the respective ML models
- Sends model training requests to the CAP4C and tracks the Machine Learning (ML) models that CAP4C builds

Analytics Subscription Service
Enables service consumers to subscribe or unsubscribe to different analytics from the OCNWDAF. It handles all the subscription requests from the consumers and updates or cancels the subscription requests from the consumers. The subscription service sends notifications to the NFs, AFs, and OAM when the subscribed event occurs in the network.

Analytics Information Service

This service enables consumers to request and obtain different analytics information from the OCNWDAF based on the 3GPP defined AnalyticsInfo API. This service is based on the REST API request-response model. This service handles the request for analytics based on the AnalyticsID. The service responds to the request and provides the analytics information if the requested analytics information is available.

Data Collection

The OCNWDAF retrieves data from various sources (for example, NFs such as AMF and SMF). Network analytics is computed using this data. The Data Collection Controller and Data Collection microservices perform data collection for the OCNWDAF. These microservices ensure the OCNWDAF obtains the appropriate data with the proper granularity.

- **Data Collection Controller Service**: This service subscribes to all NFs, manages the subscriptions, and updates the Analytics Subscription service. It also manages and prioritizes data collection between 3GPP NFs and the Data Director (OCNADD). The OCNADD has a higher priority than the 3GPP NFs.
- **Data Collection Service**: This service collects data from the producer NFs and streams it to the CAP4C for further processing.

NRF Client Service

NRF Client integrates with the NRF for OCNWDAF registration, discovery, and service status or load information, along with application and performance information services. NRF discovery helps in the on-demand discovery of network functions. NRF management helps in the autonomous discovery of NFs.

Redundancy Agent

This microservice maintains communication and controls responsibilities between the mated sites in a georedundant deployment. If there are more than two sites, then the Redundancy Agent is responsible for assigning the hierarchy of control.

Capex Service

This microservice processes the available data and identifies metrics like the active UEs per cell and the aggregated tracking area, the user plane resources (the UPFs) servicing the tracking area, and optionally, the UPFs or AMFs or SMF NF load servicing the tracking area.

cnDBTier MySQL database

cnDBTier performs general configuration, stores microservice data including dynamic data such as states, subscriptions, work lists, and data used for reporting.

Analytics database

This database is based on the MySQL cluster and stores relational and time-series data. The relational data represents all the objects within the telecommunication network, such as UEs, slices, cells, NFs, and so on, and their relationships with each other. The time-series data represents all the KPIs, measurements, and event data collected over time and used in streaming analytics and training ML models.

Kafka

A reliable and scalable distributed event streaming platform. It is used for internal as well as external delivery and consumption of data and events. It exports special measurements and events to external consumers. It also imports measurements and events from operator sources such as a messaging bus and data lake.

Stream Processors

Cleans, merges, and splits data as required and examines data in windows to detect threshold crossings or perform complex calculations.

Model Controller

Receives model generation or execution requests from the OCNWDAF FE. The Model Controller manages and allocates work to the Model Executor pool.

Model Executor

The Model Executor accesses the information in the database based on the instructions received by the Model Controller and trains the ML models.

OCNWDAF Portal

Performs the following functions:

- Manages the OCNWDAF dashboards
- Accepts operator input for configuration such as adding new network slices, geofences, and so on.
- Provides visualization of analytics information

3
OCNWDAF Features

This section explains the OCNWDAF features.

3.1 Support for Model C Communication

5G Service Based Interface (SBI) communication models are used to establish connections among NFs and NF services. These communication models facilitate consumer NFs to route service requests to producer NFs either directly or indirectly through the Service Communication Proxy (SCP). For more information about different communication models, such as Model A, Model B, Model C, and Model D, see 3GPP TS 23.501 version 16.6.0 Release 16.

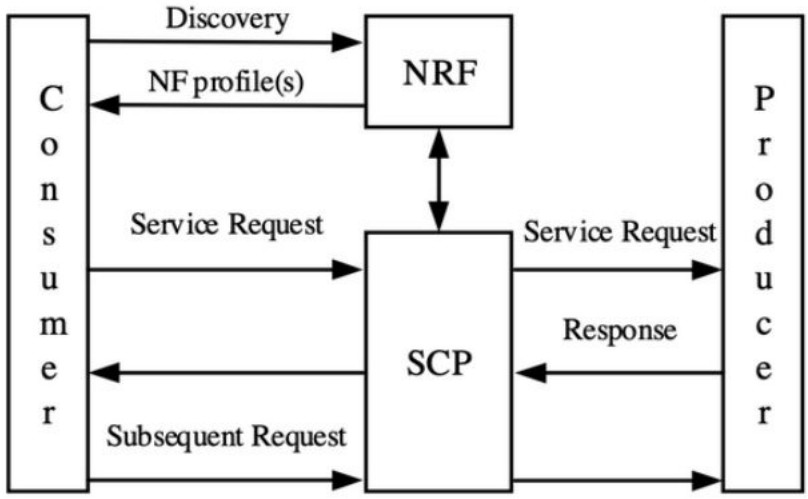
The OCNWDAF supports the Model C communication model. The SCP is located between the OCNWDAF and the producer NFs, and data is collected from them.

Model C is an indirect communication model in which consumers can query the NRF to perform NF discovery (delegated discovery) or the consumers can directly send service requests to the SCP without NRF discovery. The consumer selects a specific NF instance from an NF set from the discovery result and sends a request to the SCP, which performs all the routing. The SCP also interacts with NRF to obtain selection parameters such as location, capacity, and so on. The SCP routes the service request to the selected NF service producer instance, gathers the response, and forwards it to the consumer OCNWDAF.

Model C model can also be implemented without the NRF performing NF discovery. In this case, the OCNWDAF sends a service request to the SCP, which in turn forwards the request directly to the target NF producer. The SCP forwards the response received from the NF producer to the OCNWDAF. The communication between the OCNWDAF, SCP, and the producer NF is established by the “3gpp-Sbi-Target-apiRoot” header introduced for Model C communication. To enable or disable this feature, see *Oracle Communications Networks Data Analytics Function Installation, Upgrade, and Fault Recovery Guide*.

The diagram below depicts the implementation of Model C communication by OCNWDAF:

Figure 3-1 Model C Communication



> **Note**
>
> - The consumer in this context is OCNWDAF.
> - Producers include all external NFs such as AMF, SMF, OAM, and so on.
> - The NRF contains all the NFs' profile information and informs OCNWDAF about the valid NF from which it can collect information. The discovery function is delegated to the NRF.
> - The SCP is a proxy between the external NFs and OCNWDAF.

Support for Binding Headers in Model C Indirect 5G SBI Communication

OCNWDAF supports the following 5G SBI custom header in Model C Indirect 5G SBI Communication:

- 3gpp-Sbi-Binding: This header contains a comma-delimited list of Binding Indications from an HTTP server for storage and use of HTTP clients. The absence of this parameter in a Binding Indication in a service request is interpreted as "callback".

OCNWDAF does not update the value of the "3gpp-Sbi-Binding" header in the HTTP/2 request or response.

> **Note**
>
> Binding level NF service Set and NF service instance are not supported.

To enable OCNWDAF support for binding headers, set the `models.binding` parameter as follows:

```
modelc:
  binding:
    enabled: true
```

3.2 Support for TLS 1.3

Network Functions (NFs) or peers use Hypertext Transfer Protocol Secure (HTTPS) to establish secured ingress and egress connections with consumer NFs and producer NFs, respectively. These communication protocols are encrypted using Transport Layer Security (TLS). The OCNWDAF now supports TLS version 1.3.

TLS comprises the following components:

- **Handshake Protocol**: Exchanges the security parameters of a connection. Handshake messages are supplied to the TLS record layer.
- **Record Protocol**: Receives the messages to be transmitted, fragments the data into multiple blocks, secures the records, and then transmits the result. Received data is delivered to higher-level peers.

Gateway Services are integrated with OCNWDAF to support TLS 1.3 on the Ingress and Egress interfaces.

This feature enables the support for TLS 1.3 for all functions and interfaces where TLS 1.2 was supported. TLS 1.2 will continue to be supported.

The following table provides comparison of TLS 1.2 with TLS 1.3:

Table 3-1 Comparison of TLS 1.2 and TLS 1.3

Feature	TLS 1.2	TLS 1.3
TLS Handshake	• The initial handshake was carried out in clear text. • A typical handshake in TLS v1.2 involved the exchange of 5 to 7 packets.	• The initial handshake is carried out along with the key share. • A typical handshake IN TLS v1.3 involves the exchange of up to 3 packets.
Cipher Suites	• Less secure Cipher suites. • Used SHA-256 and SHA-384 hashing	• More secure Cipher suites. – TLS_CHACHA20_POLY1305_SHA256 – TLS_AES_128_GCM_SHA256 – TLS_AES_256_GCM_SHA384 – TLS_AES_128_CCM_8_SHA256 – TLS_AES_128_CCM_SHA25 **Note:** At present, the two CCM ciphers mentioned above are not supported by Java library.
Round-Trip Time (RTT)	This has a high RTT during the TLS handshake.	This has low RTT during the TLS handshake.
Perfect Forward Secrecy (PFS)	This doesn't support PFS.	TLS V1.3 supports PFS. PFS ensures that each session key is completely independent of long-term private keys, that are used for an extended period to decrypt encrypted data.

Table 3-1 (Cont.) Comparison of TLS 1.2 and TLS 1.3

Feature	TLS 1.2	TLS 1.3
Privacy	This is less secure as the ciphers used are weak.	This is more secure as the ciphers used are strong.
Performance	This has high latency and a less responsive connection.	This has low latency and a more responsive connection.

TLS 1.3 handshake offers the following improvements over earlier versions:

- The symmetric encryption algorithms are removed and Authenticated Encryption with Associated Data (AEAD) algorithms are supported.
- In TLS 1.3, all handshake messages after the ServerHello is encrypted.
- TLS 1.3 improves efficiency in the handshake process by requiring fewer round trips than TLS 1.2. It also uses cryptographic algorithms that are faster.
- TLS 1.3 has better security than TLS 1.2. It addresses known vulnerabilities in the handshake process.
- Zero Round-Trip Time (0-RTT) key exchanges streamline the TLS handshake better.
- TLS 1.3 got rid of data compression.
- Version Downgrade Protection in TLS v1.3 is a security mechanism that prevents attackers from using an older, potentially less secure version of the TLS protocol. This protection is achieved through the exchange of a "Finished" message between the client and server, which includes a Message Authentication Code (MAC) covering all preceding handshake messages. This mutual verification process ensures that negotiated parameters remain unaltered by potential attackers. This helps ensure that connections are established using the latest, most secure version of TLS available, reducing the risk of vulnerabilities associated with older protocol versions.

The following digital signature algorithms of TLS 1.2 and TLS 1.3 are supported in TLS handshake:

Table 3-2 Algorithms

Algorithm	Key Size (Bits)	Elliptic Curve (EC)
RS256 (RSA)	2048	NA
	4096 This is the recommended value.	NA
ES256 (ECDSA)	NA	SECP384r1 This is the recommended value.

Note

The following functionalities are not supported:

- Zero round-trip time (0-RTT) mode
- Pre Shared Key (PSK) exchange

Configure

You can configure this feature using Helm parameters. Configure the following parameters in the Ingress Gateway and Egress Gateway, required for TLS1.3:

```
clientDisabledExtension: ec_point_formats #comma-separated-values To disable
extension being sent in ClientHello
serverDisabledExtension: null #comma-separated-values To disable extension
being sent from server originated messages
tlsNamedGroups: null #comma-separated-values to whitelist the
supported_groups extension values
clientSignatureSchemes: null #comma-separated-values to whitelist the
signature_algorithms extension values
service:
  ssl:
    tlsVersion: TLSv1.2,TLSv1.3
allowedCipherSuites:
  - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
  - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
  - TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
  - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
  - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
  - TLS_AES_256_GCM_SHA384
  - TLS_AES_128_GCM_SHA256
  - TLS_CHACHA20_POLY1305_SHA256
cipherSuites:
  - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
  - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
  - TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
  - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
  - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
  - TLS_AES_256_GCM_SHA384
  - TLS_AES_128_GCM_SHA256
  - TLS_CHACHA20_POLY1305_SHA256
```

> **Note**
>
> - If you want to provide values for the signature_algorithms extension using the `clientSignatureSchemes` parameter, the following comma-separated values must be provided to deploy the pods:
>   - rsa_pkcs1_sha512
>   - rsa_pkcs1_sha384
>   - rsa_pkcs1_sha256
> - The mandatory extensions as listed in RFC 8446 cannot be disabled on the client or server side. The following is the list of the extensions that cannot be disabled:
>   - supported_versions
>   - key_share
>   - supported_groups
>   - signature_algorithms
>   - pre_shared_key

To configure TLS 1.3 support, see *Oracle Communications Networks Data Analytics Function Installation, Upgrade, and Fault Recovery Guide*.

3.3 Capex Optimization

In a network, subscribers are distributed unevenly, resulting in some areas having high density of subscribers as compared to others. Areas with a high density of subscribers require additional resources. The Capex Optimization service identifies such regions based on the information about preferred subscribers and network activity in that area. OCNWDAF collects information about the active UEs per cell, the aggregated tracking area, the user plane resources serving in the tracking area, and the NFs (UPF or, AMF or SMF) load servicing (optionally) the tracking area to determine severely congested tracking areas and derive Capex metrics about the preferred subscribers in a group for a tracking area.

For information on the Capex Optimization microservice, see Capex Optimization Service.

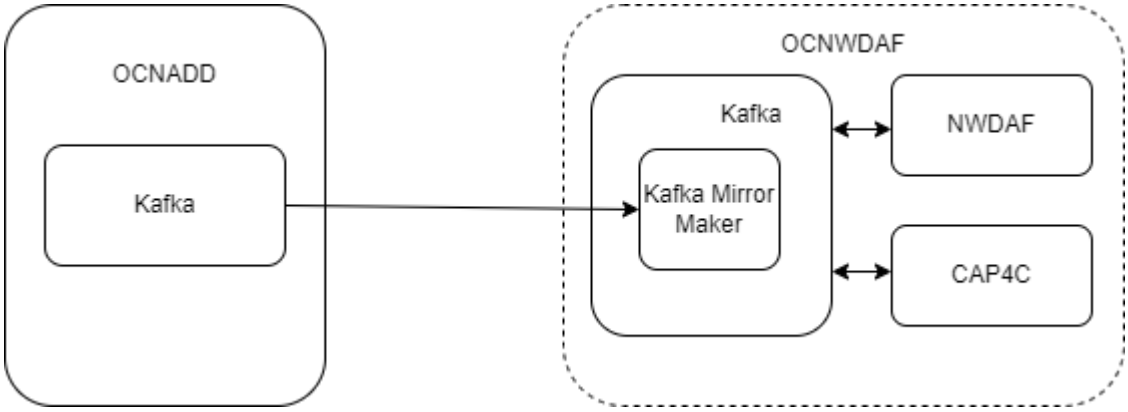
The user can create Capex groups using the OCNWDAF GUI and view the Capex Analytics on the GUI. For more information, see Capex Optimization.

3.4 Data Director (OCNADD) Integration

The OCNWDAF supports the Oracle Communications Network Analytics Data Director (OCNADD) as a data source. The Kafka Mirror Maker replication utility replicates Kafka topics between the OCNADD and the OCNWDAF. A Helm parameter *dataSource* is introduced in the *values.yaml* file to enable (or disable) OCNADD as a data source.

> **Note**
>
> The Slice Load Level Analytics, UE Mobility Analytics, and UE Abnormal Behavior Analytics can be derived when the OCNADD is configured as a data source.

Figure 3-2 Kafka Replication



For information on prerequisites to enable this feature, see "Environment Setup Requirements" section in *Oracle Communications Networks Data Analytics Function Installation, Upgrade, and Fault Recovery Guide*.

To enable OCNADD as a data source, see "Configure Data Director" and "Installing OCNWDAF Package" sections in *Oracle Communications Networks Data Analytics Function Installation, Upgrade, and Fault Recovery Guide*.

3.5 Machine Learning (ML) Model Evaluation and Selection

Machine Learning (ML) models are programs trained to identify patterns within data sets. Data sets contain historical data and vary based on region, use case, and service provider. ML algorithms analyze and detect patterns within a data set to train ML models. Trained ML models predict analytics based on the input data.

Algorithms are selected based on the data set and use case. Accordingly, different algorithms are effective in distinct scenarios. To obtain accurate predictions, users must retrain the ML models frequently. Users have flexibility in selecting, optimizing, testing, and training ML models.

The OCNWDAF provides a GUI dashboard to select, train, and optimize one or more ML Models for a given analytics category. The user can select among multiple algorithms supported by each analytics category and run experiments to determine the best-suited ML model for each data set. ML models are evaluated by running experiments and metrics are generated. Metrics for each experiment is displayed on the dashboard. User can select the ML model based on these metrics. Multiple algorithms can be selected simultaneously to run experiments.

To access the ML Model Selector page and perform ML model evaluation on the OCNWDAF GUI, see Machine Learning (ML) Model Selector.

3.6 Network Performance Visualization on the OCNWDAF Dashboard

The OCNWDAF provides network performance analytics to the consumer. The analytics information primarily includes resource consumption by gNodeB (gNB) and mobility performance indicators in the Area of Interest (AoI). The users can access the following network performance analytics on the OCNWDAF GUI:

- All available cells in a selected Tracking Area
- For each cell, the user can view the following information:
  - GNB Computing, Memory, and Disk Usage
  - Session Success Ratio
  - HO Success Ratio
- The user can set a threshold value, select a tracking area and a time interval in the GUI. All the available cells in the selected tracking area within the selected time interval and specified threshold value are displayed on the screen.

For more information, see Monitoring page in the OCNWDAF GUI.

3.7 Service Mesh for Intra-NF Communication

OCNWDAF leverages the service mesh support for all internal and external communication. The service mesh integration provides intra-NF communication and allows API gateway coworking with service mesh. The service mesh integration supports the services by deploying a special sidecar proxy in the environment to intercept all network communication between microservices.

> **Note**
>
> For service mesh integration, the service mesh must be available in the cluster in which OCNWDAF is installed.

For more information about configuring service mesh, see *Oracle Communications Networks Data Analytics Function Installation, Upgrade, and Fault Recovery Guide*.

3.8 Georedundancy

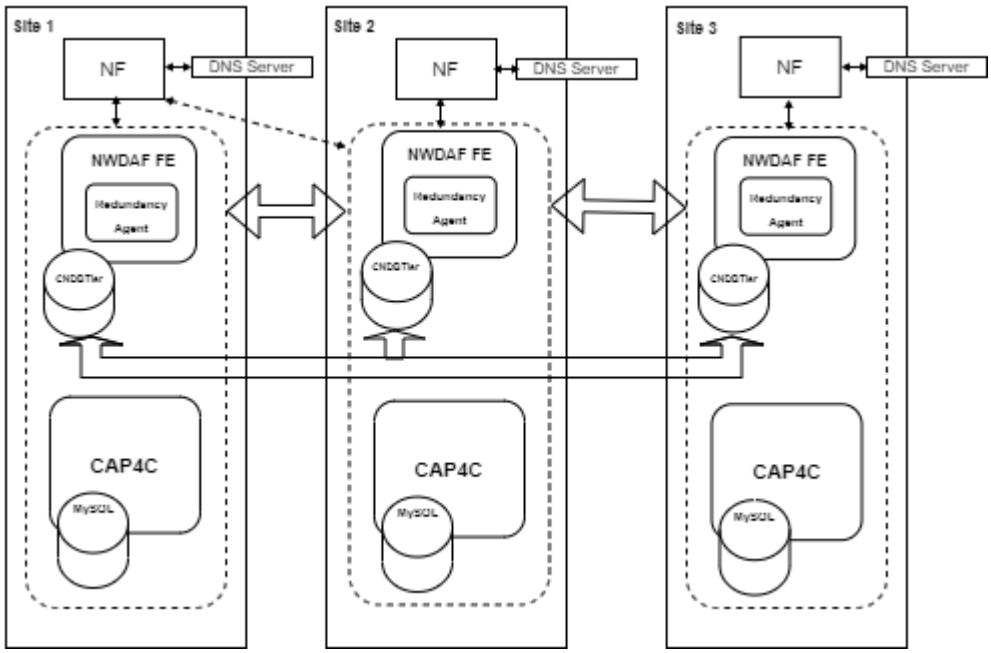
Overview

A network includes multiple sites, and each site can be located at different data centers and spread across geographic locations. A network failure can occur due to reasons such as outages, software defects, hardware issues, and so on. These failures impact the continuity of network services. Georedundancy is used to mitigate such network failures and ensure service continuity. In a georedundant deployment, when a failure occurs at one site, an alternate site takes ownership of all the subscriptions and activities of the failed site. The alternate site ensures consistent data flow, service continuity, and minimal performance loss. Georedundancy includes implementing data replication of one site across multiple sites to efficiently handle failure scenarios and ensure High Availability (HA). OCNWDAF along with data replication supports Machine Learning (ML) Model replication.

Georedundant Deployment Architecture

The OCNWDAF supports both 2-site and 3-site georedundant deployments. The following diagram depicts a 3-site georedundant deployment.

Figure 3-3 Georedundant Architecture



Redundancy Agent

Redundancy Agent is the microservice introduced to maintain communication and enable site transfer between the mated sites. It uses a heartbeat mechanism to broadcast the liveness of a site and receives liveness updates from mated sites.

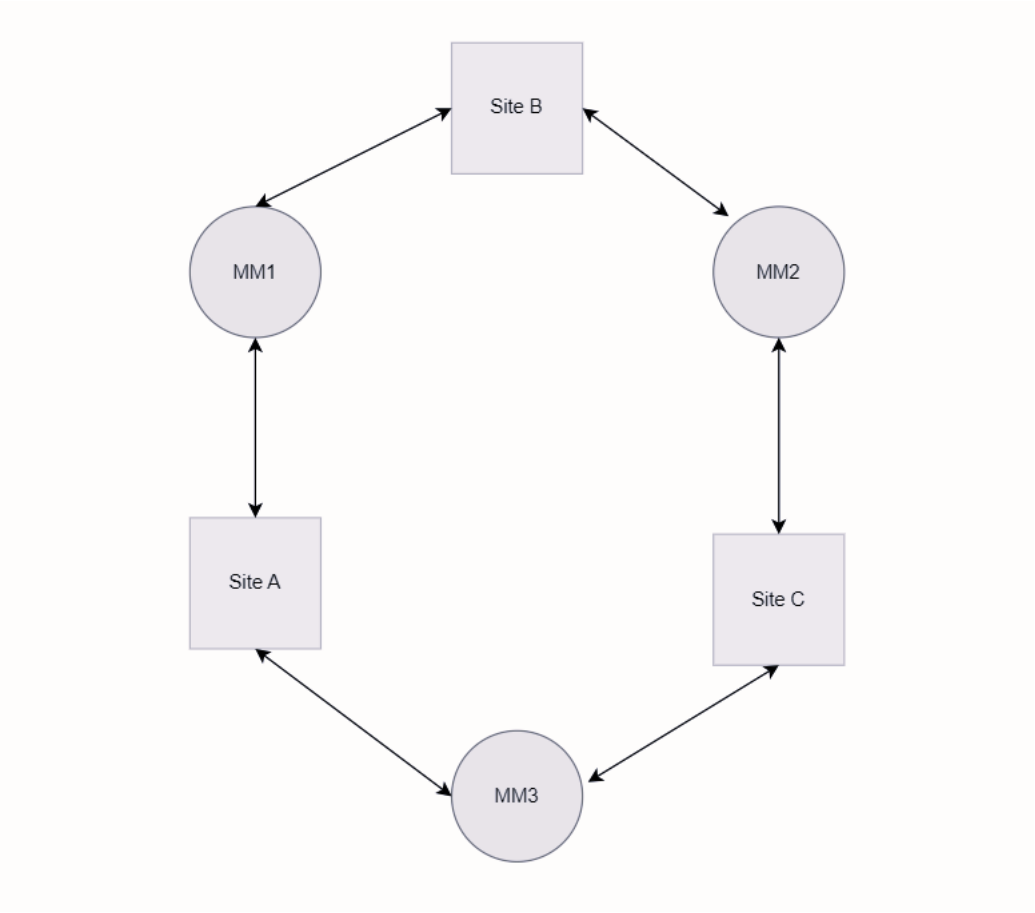
Site transfer is based on the configured priority of the mated sites. The Redundancy Agent of every site maintains a priority list of the mated sites. The priority list is configured using the Helm chart. A site can access the priority list of other sites using the database and build the ownership matrix. When a site failure occurs at the primary site, the ownership is transferred to the secondary site. If the secondary site fails, the ownership is transferred to the tertiary site and so on. Identifying and recognizing a failed site is based on a quorum, where a majority of active sites agree on the failed status of the site.

An NF sends a subscription request to the Analytics Subscription Service. The subscription service verifies if the subscription exists and if it is a new subscription, it stores the subscription data and the site ID. The Redundancy Agent accordingly responds with a status to the subscription service. If the status is ACTIVE, the Analytics Subscription Service continues with the subscription request. If the Analytics Subscription Service receives any other status, it responds to the subscription request with an HTTP 5XX response. The subscription service updates and maintains site status based on the response received by the Redundancy Agent. If a subscription request is received from a NF when the site is down, the transfer of responsibility to mated site is the addressed by the Redundancy Agents, the request is forwarded to the site that is currently handling all the subscription requests of the site that is down. If a core component failure occurs, the Redundancy Agent intimates the Subscription Service, the Subscription Service caches the data sent by Redundancy Agent, and further this data is referred by Subscription Service while accepting fresh subscriptions. The Analytics Information Service also operates like the Analytics Subscription Service. The Redundancy Agent provides the site liveness data to the Data Collection Service when there is a change in the core component status. The Data Collection Service caches the data sent by Redundancy Agent, and refers to this data while accepting fresh data collection requests.

Data Replication

In a georedundant deployment, High Availability (HA) can be achieved by data replication across all sites. Data topics across all sites are replicated by the “Mirror Maker 2 (MM2)” which is the replication tool for Kafka topics. A three-site georedundant deployment requires three MM2s to operate in a circular topology. The MM2s are located in each site's environment. The diagram below depicts the recommended circular topology for a three-site georedundant deployment:

Figure 3-4 Circular Topology

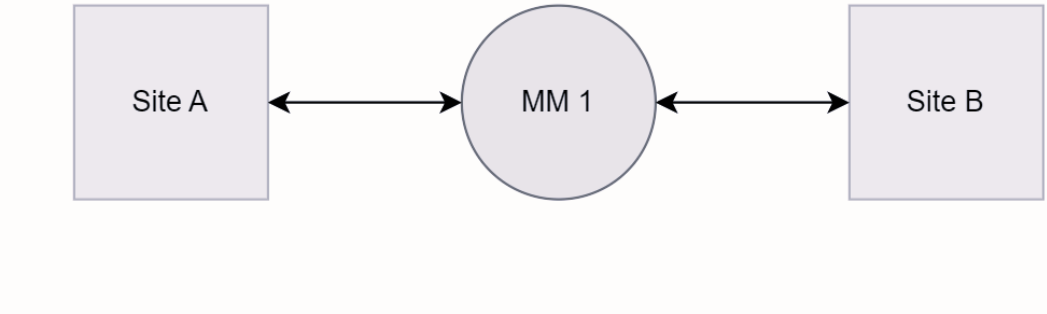


In the above diagram:

- The Mirror Maker “MM1” of Site A handles the replication for both Sites A and B.
- The Mirror Maker “MM2” of Site B handles the replication for both Sites B and C.
- The Mirror Maker “MM3” of Site C handles replication for Sites C and A.

A two-site georedundant deployment requires only one MM2 connecting the sites. The MM2 can be in either of the site's environments. The diagram below depicts the recommended topology for a two-site georedundant deployment:

Figure 3-5 Two-Site Deployment



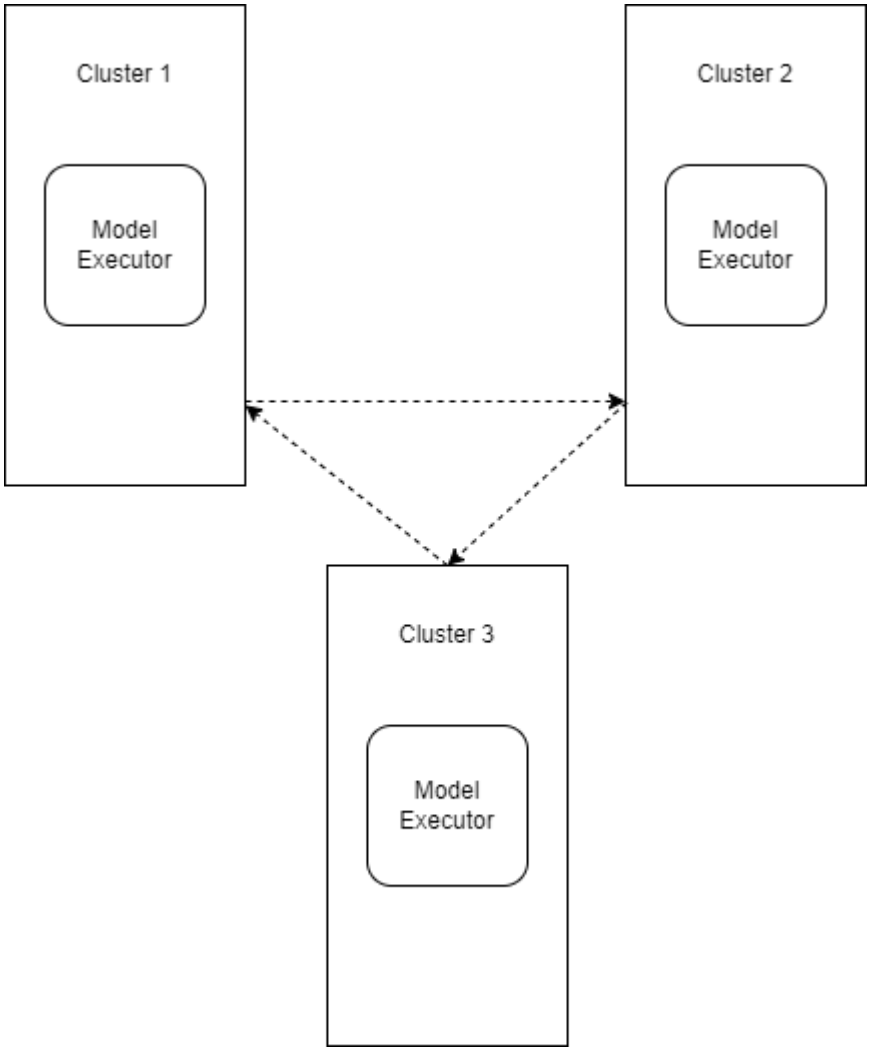
Prerequisites

- Each site configures the remote OCNWDAF sites that it shall be georedundant with.
- The data replication service must be in good health.
- Georedundant sites must be time synchronized.
- Georedundant OCNWDAF sites must be reachable from NFs from all three sites.
- The NFs register their services and maintain heartbeats with the OCNWDAF. The data is replicated across the georedundant OCNWDAFs, thereby allowing the NFs to seamlessly move between the OCNWDAFs in case of failure.
- The configurations at each site shall be the same to allow the OCNWDAFs at all sites to handle the subscriber NFs in the same manner.
- This feature is configured using Helm.
- For a three-site georedundant deployment use a circular topology with active/active connection for three sites.
- Recommended latency is less than 100 ms.

Machine Learning (ML) Model Replication

The Analytics Engine (CAP4C) collects data from the OCNWDAF's Front End (FE), performs data processing, and trains Machine Learning (ML) models. The Model Controller and Model Executor services perform these functions. The Model Controller receives model generation or execution requests from the FE. The Model Controller manages and allocates work to the Model Executor service. The Model Executor accesses the information from the database based on the instructions received by the Model Controller and trains the ML models. It trains ML models and draws inferences for all the supported Analytics IDs. In a georedundant deployment, ML models created by the Model Executor are replicated across all georedundant sites. The diagram below depicts a how the Model Executor service is replicated in a three-site georedundant deployment :

Figure 3-6 ML Model Replication



The Synchronization Tool (rsync) accesses the files created by the Model Executor service and the Load Balancer service communicates with all the clusters in the deployment.

To configure ML model replication, see *Oracle Communications Cloud Native Core Networks Data Analytics Function Installation, Upgrade, and Fault Recovery Guide*.

Georedundant Deployment Failure Scenarios

Listed below are possible failure scenarios in georedundant deployments and the respective recovery mechanisms to prevent network failures:

Table 3-3 Failure Scenarios

Failure Scenario	Recovery Mechanisms
One of the mated OCNWDAF sites is down, and the heartbeat is not exchanged.	The Redundancy Agent updates the ownership matrix and transfers site ownership to the active site based on the existing ownership matrix.

Table 3-3 (Cont.) Failure Scenarios

Failure Scenario	Recovery Mechanisms
The mated OCNWDAF site is up, but the heartbeat exchange is missed.	Redundancy Agent marks the unresponsive mated site as UNAVAILABLE and after number of heartbeats missed crosses the configured threshold, the Redundancy Agent marks the site as INACTIVE. Transfer of ownership is then initiated based on the priority list.
Heartbeats are exchanged, but the OCNWDAF site is experiencing a core component failure.	In case of core component failure, the redundancy agent uses the K8s client to identify the failure of core components. The Redundancy Agent updates the ownership matrix and transfers site ownership to the active site based on the existing ownership matrix.
cnDBTier Primary Replication Channel Failure, cnDBTier Secondary Replication Channel Failure and cnDBTier Both Replication Channel Failure	cnDBTier takes appropriate action. For more information, see, *Oracle Communications Cloud Native Core cnDBTier Installation, Upgrade, and Fault Recovery Guide*. **Note** Transferring ownership in this case may result in some data loss.
Complete cnDBTier Failure or DB Connection Failure with OCNWDAF.	Redundancy Agent updates the current status of the OCNWDAF site as **unavailable/down**, updates the ownership matrix, and sends the heartbeat to mated sites. Redundancy Agent determines the status of the DB and takes appropriate action. For more information on cnDBtier recovery, see, *Oracle Communications Cloud Native Core cnDBTier Installation, Upgrade, and Fault Recovery Guide*
NF unable to send or communicate with local OCNWDAF.	The NF uses the DNS (or SCP Model-D) to obtain the IP of the secondary site which will now be responsible for the current site.

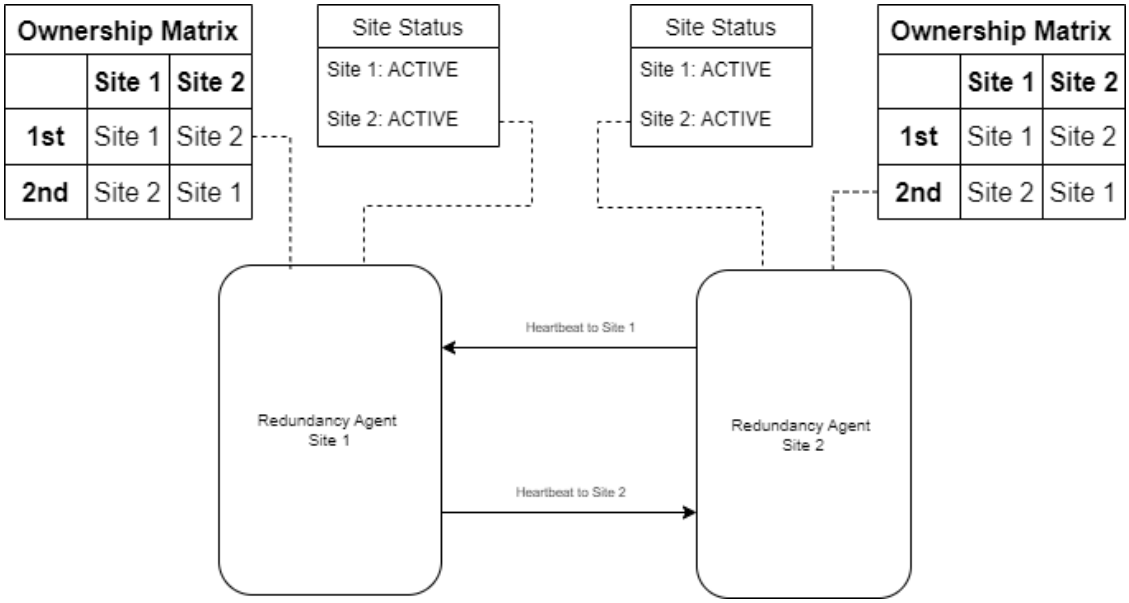
Note

- In case of cnDBTier replication channel failures or complete cnDBtier failure, see, *Oracle Communications Cloud Native Core cnDBTier Installation, Upgrade, and Fault Recovery Guide*
- When one or more core components of an OCNWDAF instance fails, the OCNWDAF instance marks itself as INACTIVE, and broadcasts this message to other mated sites. The mated sites initiate the ownership transfer process.

Two-Site Georedundancy

The following diagram depicts a two-site georedundant deployment:

Figure 3-7 Two-Site Georedundancy



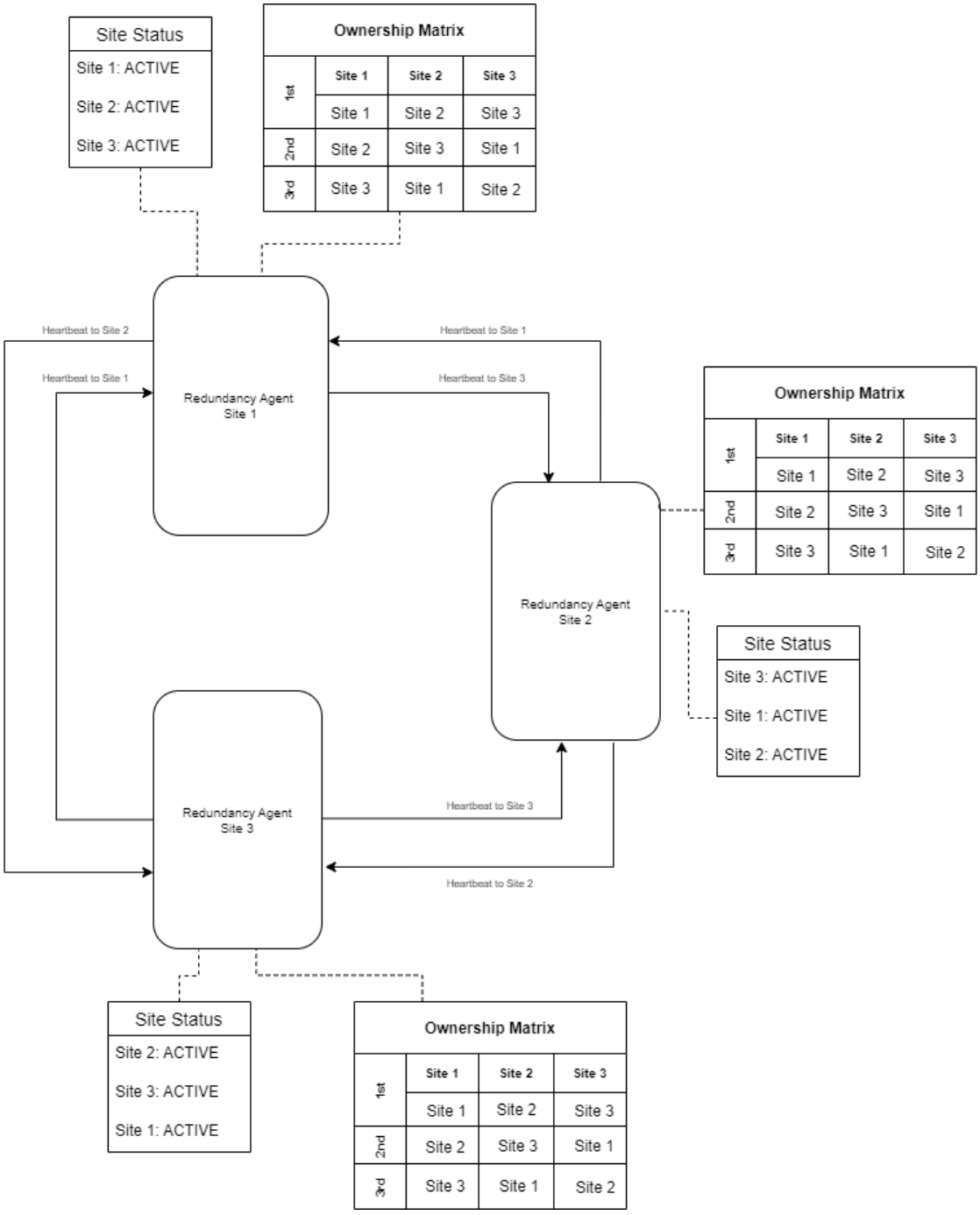
The ownership matrix determines the transfer of ownership when a site failure occurs. The site failure is determined by the site status. The site status can be ACTIVE, INACTIVE, SUSPENDED, DISCOVERY and UNAVAILABLE. The ownership transfer occurs as per the ownership matrix when the site is INACTIVE, SUSPENDED or UNAVAILABLE.

For example, when Site 2 is INACTIVE, based on the ownership matrix Site 1 becomes the owner of all subscriptions owned by Site 2.

Three-Site Georedundancy

The following diagram depicts a three-site georedundant deployment:

Figure 3-8 Three-Site Georedundancy



The ownership matrix determines the transfer of ownership when a site failure occurs. The site failure is determined by the site status. The site status can be ACTIVE, INACTIVE, SUSPENDED, DISCOVERY and UNAVAILABLE. The ownership transfer occurs as per the ownership matrix when the site is INACTIVE, SUSPENDED or UNAVAILABLE.

For example, when Site 1 is down, Site 2 takes ownership of the subscriptions at Site 1. If Site 2 is also down Site 3, assumes ownership of subscriptions at Site 1. The transfer of ownership is based on the priority configured in the Ownership Matrix.

Managing Georedundancy

Deploy

To deploy OCNWDAF in a georedundant environment:

- Install cnDBTier version 22.4.0 or above on each configured site. Ensure the DB Replication Channels between the sites are UP. For information about installing cnDBTier, see "Installing cnDBTier" in *Oracle Communications Cloud Native Core cnDBTier Installation, Upgrade, and Fault Recovery Guide*.
- Deploy OCNWDAF over the replicated cnDBTier sites. Ensure the sites have different names. For information about installing and deploying OCNWDAF, see *Oracle Communications Cloud Native Core Networks Data Analytics Function Installation Guide and Fault Recovery Guide.*
- Ensure that the redundancy agent details are added to the common gateway routing rules.

To install the Mirror Maker for data replication, see *Oracle Communications Cloud Native Core Networks Data Analytics Function Installation, Upgrade, and Fault Recovery Guide*.

Configure Georedundancy

To configure the Redundancy agent, see the section *"Configure Redundancy Agent" in Oracle Communications Cloud Native Core Networks Data Analytics Function Installation Guide and Fault Recovery Guide.*

Configure the georedundancy specific parameters in the OCNWDAF instances on the replicated sites. Configure the following parameters in the redundancy agents properties file to enable and configure georedundancy in the deployed sites:

- Set the **GEO_REDUNDANCY_ENABLE** parameter to true.
- Ensure that the following parameters are properly configured (based on number of georedundant sites in the deployment) in the redundancy agents properties file:
  - **GEO_RED_AGENT_SITE_SECONDARY_SITEID**
  - **GEO_RED_AGENT_SITE_SECONDARY_ADDRESS**
  - **GEO_RED_AGENT_SITE_TERTIARY_SITEID**
  - **GEO_RED_AGENT_SITE_TERTIARY_ADDRESS**
  - **GEO_RED_SITE_SELF_PRIORITY**
  - **GEO_RED_AGENT_SITE_ID**
  - **GEO_RED_AGENT_SELF_ADDRESS**
  - **GEO_RED_AGENT_NUMBER_OF_MATED_SITE**

  For example:

  ```
  GEO_RED_AGENT_NUMBER_OF_MATED_SITE: 2
  GEO_RED_AGENT_SITE_SECONDARY_SITEID: OCNWDAF-XX-2
  GEO_RED_AGENT_SITE_SECONDARY_ADDRESS: http://ocn-nwdaf-gateway-service:8088
  GEO_RED_AGENT_SITE_TERTIARY_SITEID: OCNWDAF-XX-3
  GEO_RED_AGENT_SITE_TERTIARY_ADDRESS: http://ocn-nwdaf-gateway-service:8088
  ```

- If the deployment is a two-site georedundant deployment the tertiary site is not a part of the georedundant deployment, set a placeholder value. It should not be empty.

- After OCNWDAF instances are deployed over replicated cnDBTier sites, run the following command:

  ```
  helm install {releasename} {chartlocation} -n
      {namespace}
  ```

  For example:

  ```
  helm install grdagent charts -n nwdaf
  ```

Configure the following parameters to enable and configure georedundancy in the custom values file for OCNWDAF:

Table 3-4 REDUNDANCY AGENT CONFIGURATION

Parameter	Description	Default Value
ocnwdaf.cluster.namespace	Name space of the deployment **Note:** Change this to the name space of OCNWDAF deployments.	ocn-nwdaf
global.ocnNwdafGeoredagent	This parameter enables the georedundancy feature, it is turned off by default. Set this parameter to "True" to enable georedundancy.	False
global.siteVariables.OCNWDAF_SITE_ID	This parameter sets the name of the Site, it is used by the redundancy agent, the scheduler service, and the subscription service.	OCNWDAF-XX-1
ocnnwdaf.geored.hooks.database	Database information for the hook	nwdaf_subscription
ocnnwdaf.geored.hooks.table	Table information for the hook	nwdaf_subscription
ocnnwdaf.geored.hooks.column1	Column1 information for the hook	record_owner
ocnnwdaf.geored.hooks.column2	Column2 information for the hook	current_owner
ocnnwdaf.geored.hooks.image	Image information for the hook	ocnwdaf-docker.dockerhub-phx.oci.oraclecorp.com/nwdaf-cap4c/nwdaf-cap4c-mysql:8.0.30
ocnnwdaf.geored.agent.name	Name of the deployment	ocn-nwdaf_georedagent
ocnnwdaf.geored.agent.replicas	Number of Replicas	1
ocnnwdaf.geored.agent.image.source	Image for GRD Agent **Note:** Modify this value if the image is in a different repository.	occne-repo-host:5000/occne/redagent-ms-dev:1.0.31
ocnnwdaf.geored.agent.image.pullPolicy	Image Pull Policy	IfNotPresent
ocnnwdaf.geored.agent.resources.limits.cpu	CPU Limit	1
ocnnwdaf.geored.agent.resources.limits.memory	Memory Limit	1Gi
ocnnwdaf.geored.agent.resources.request.cpu	CPU Request	1

Table 3-4 (Cont.) REDUNDANCY AGENT CONFIGURATION

Parameter	Description	Default Value
ocnnwdaf.georedagent.resources.request.memory	Memory Request	1Gi
ocnnwdaf.georedagent.service.type	Service Type of the Deployment	ClusterIP
ocnnwdaf.georedagent.service.port.containerPort	Container Port of the Deployment	9181
ocnnwdaf.georedagent.service.port.targetPort	Target Port of the Deployment	9181
ocnnwdaf.georedagent.service.port.name	Name of the Service Port	ocnwdafgeoredagentport
ocnnwdaf.georedagent.service.prometheusport.containerPort	Container Port of the Prometheus	9000
ocnnwdaf.georedagent.service.prometheusport.targetPort	Target Port of the Prometheus	9000
ocnnwdaf.georedagent.service.prometheusport.name	Name of the Prometheus **Note:** Modify the port name based on the promethus on the deployed setup.	http-cnc-metrics
ocnnwdaf.georedagent.env.GEO_RED_AGENT_SERVER_HTTP2_ENABLED	Enable/Disable HTTP2	TRUE
ocnnwdaf.georedagent.env.GEO_RED_AGENT_HEARTBEAT_INTERVAL_MS	Time Interval To check HeartBeat in "ms"	10000
ocnnwdaf.georedagent.env.GEO_RED_AGENT_HEARTBEAT_THRESHOLD	Number of Time Times to check Heart Beat	5
ocnnwdaf.georedagent.env.GEO_RED_AGENT_CORE_COMP_THRESHOLD	Number of Time Times to check Heart Beat toward Core Components provides	5
ocnnwdaf.georedagent.env.GEO_RED_AGENT_SITE_NUMBER	Current Site Number	1
ocnnwdaf.georedagent.env.GEO_RED_AGENT_SITE_ID	Current Site ID	OCNWDAF-XX-1
ocnnwdaf.georedagent.env.GEO_RED_AGENT_NUMBER_OF_MATED_SITE	Number of Mated Sites. It is updated based on GRD Sites in sync.	1
ocnnwdaf.georedagent.env.GEO_RED_AGENT_SELF_ADDRESS	Current Agent Address. The resolvable URL of the OCNNWDAF Gateway service. This address should be reachable outside the cluster .	
ocnnwdaf.georedagent.env.GEO_RED_AGENT_MICROSERVICE_LIVELINESS_MS	Check Interval for OCNWDAF Microservice in "ms".	10000
ocnnwdaf.georedagent.env.GEO_RED_AGENT_OCNWDAF_CORE_COMPONENT_LIST	List of OCNWDAF microservices that needs to be verified.	ocn-nwdaf-subscription
ocnnwdaf.georedagent.env.GEO_RED_SITE_SUBSCRIPTION_OWNERSHIP_TRANSFER_URL	Subscription API for Ownership Transfer	http://ocn-nwdaf-subscription-service-internal:8087/nnwdaf-eventssubscription/v1/subscriptions/updateServingOwner

Table 3-4 (Cont.) REDUNDANCY AGENT CONFIGURATION

Parameter	Description	Default Value
ocnnwdaf.geored.agent.env.GEO_RED_SITE_DATA_COLLECTION_URL	Data Collection API for Ownership Check	http://ocn-nwdaf-data-collection-service-internal:8081/ra/notify
ocnnwdaf.geored.agent.env.GEO_RED_AGENT_DBTIER_REPLICATION_STATUS_URL	cnDBTier Monitor Service URL for Replication	Use the Reachable Monitor Service from Deployed CNDB namespace. For example: http://mysql-cluster-db-monitor-svc.{cndbnamspace}.svc.{domainname}:8080/db-tier/status/replication
ocnnwdaf.geored.agent.env.GEO_RED_AGENT_DBTIER_STATUS_URL	cnDBTier Monitor Service URL for Local	Use the Reachable Monitor Service from Deployed CNDB namespace. For example: http://mysql-cluster-db-monitor-svc.{cndbnamspace}.svc.{domainname}:8080/db-tier/status/local
ocnnwdaf.geored.agent.env.GEO_RED_AGENT_SITE_SECONDARY_SITEID	Secondary Site ID	OCNWDAF-XX-2
ocnnwdaf.geored.agent.env.GEO_RED_AGENT_SITE_SECONDARY_ADDRESS	Secondary Site Address	The Resolvable URL of the OCNWDAF Gateway of Secondary Site. This address should be reachable outside the cluster
ocnnwdaf.geored.agent.env.GEO_RED_AGENT_SITE_TERTIARY_SITEID	Tertiary Site ID	OCNWDAF-XX-3
ocnnwdaf.geored.agent.env.GEO_RED_AGENT_SITE_TERTIARY_ADDRESS	Tertiary Site Address	The Resolvable URL of the OCNWDAF Gateway of Tertiary Site. This address should be reachable outside the cluster

Table 3-4 (Cont.) REDUNDANCY AGENT CONFIGURATION

Parameter	Description	Default Value
ocnnwdaf.geored.agent.env.GEO_RED_AGENT_DB_URL	IP of the Site cnDBTier	The Cluster IP/ External IP of the CNDB
ocnnwdaf.geored.agent.env.GEO_RED_AGENT_USERNAME	Name of the DB User with privileges to GRD DB and Subscription DB. The user should have access to both GRD and Subscription Databases	occneuser
ocnnwdaf.geored.agent.env.GEO_RED_AGENT_PASSWORD	Password for the DB User	password
ocnnwdaf.geored.agent.env.GEO_RED_AGENT_ENABLE	Enable/Disable GRD	false
ocnnwdaf.geored.agent.env.GEO_RED_AGENT_DB_PORT	Port of the DB	3306
ocnnwdaf.geored.agent.env.GEO_RED_AGENT_DB_NAME	Name of the GRD Database	georedagent
ocnnwdaf.geored.agent.env.GEO_RED_AGENT_CONFIG_SERVER	Config Server URL for the Site's OCNWDAF	http://nwdaf-cap4c-spring-cloud-config-server:8888

To customize the Mirror Maker configuration for data replication, see *Oracle Communications Networks Data Analytics Function Installation, Upgrade, and Fault Recovery Guide*.

Listed below are the Mirror Maker configuration parameters:

Table 3-5 Mirror Maker Parameters

Parameter	Description
clusters	The clusters name.
clusterX.bootstrap.servers	This parameter refers to the brokers that belong to the cluster, host, and port. Multiple brokers can be separated by a comma, and clusterX is replaced by each cluster name.
clusterX.config.storage.replication.factor	The replication factor is used when Kafka Connect creates a topic to store the connector and task configuration data. This value should always be a minimum of “3” for a production system. It cannot exceed the number of Kafka brokers in the cluster. Set the value of this parameter to “1” to use the Kafka broker's default replication factor.
clusterX.offset.storage.replication.factor	The replication factor is used when Kafka Connect creates a topic to store the connector offsets. This value should always be a minimum of “3” for a production system. It cannot exceed the number of Kafka brokers in the cluster. Set the value of this parameter to “1” to use the Kafka broker's default replication factor.

Table 3-5 (Cont.) Mirror Maker Parameters

Parameter	Description
clusterX.status.storage.replication.factor	The replication factor is used when Kafka Connect creates a topic to store the connector and task status updates. This value should always be a minimum of “3” for a production system. It cannot exceed the number of Kafka brokers in the cluster. Set the value of this parameter to “1” to use the Kafka broker's default replication factor.
replication.factor	Indicates the number of brokers available.
nwdafDataReplication.config.serviceN.kafkaService	The Kafka service name to build Kafka service's FQDN.
nwdafDataReplication.config.serviceN.namespace	The namespace to build Kafka service's FQDN.
nwdafDataReplication.config.serviceN.cluster	The cluster to build Kafka service's FQDN.

Procedure to Migrate From Two-Site Georedundancy to Three-Site Georedundancy

To deploy a tertiary site in a two-site georedundant environment, update tertiary site parameters in the redundancy agents properties file.

- Update the parameters **GEO_RED_AGENT_SITE_TERTIARY_SITEID**, **GEO_RED_AGENT_SITE_TERTIARY_ADDRESS, GEO_RED_SITE_SELF_PRIORITY** to include the new site in the priority list and the address list for all sites including the existing sites and the new site as well.
- Update **GEO_RED_AGENT_NUMBER_OF_MATED_SITE** parameter in the helm chart to increase the number of mated sites to 3 for all sites.
- Configure and deploy georedundancy service on each site. Run the following command:

```
helm install {releasename} {chartlocation} -n
    {namespace}
```

Disable Georedundancy

To disable georedundancy set the **ENABLE_GEO_REDUNDANCY** parameter to false in the redundancy agents properties file.

Uninstall Mirror Maker

To unistall Mirror Maker, run the following command:

```
helm uninstall nwdaf-data-replication
```

Remove a OCNWDAF site from a Georedundant Deployment

Prerequisites

Disable replication on the CNDB MySQL Cluster. For more information see the procedure to Gracefully stop geo-replication in the *Oracle Communications Cloud Native Core cnDBTier User Guide*.

Perform the following steps:

- Remove the OCNWDAF site from the DNS Service List.

- Delete the georedundant service from the site and remove the database from sites CNDB database.
- Remove the site references from other sites and upgrade their Redundancy Agents. For example: If Site 3 is being removed, remove the reference of Site 3 from both Site 1 and Site 2 Redundancy Agents and upgrade the services.

3.9 Automated Test Suite Support

OCNWDAF provides Automated Test Suite (ATS) for validating the functionalities. ATS allows you to run OCNWDAF test cases using an automated testing tool, and then compares the actual results with the expected or predicted results. In this process, there is minimal user intervention.

For more information on installing and configuring ATS, see *Oracle Communications Network Analytics Suite Automated Test Suite Guide*.

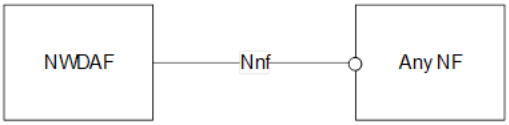
4
OCNWDAF Interfaces

This chapter describes the OCNWDAF interfaces, which are used by consumer NFs and OCNWDAF for subscription data and analytics collection.

4.1 OCNWDAF Data Collection from NFs

The OCNWDAF collects data from 5G NFs (the OCNWDAF and the NF providing the data belong to the same PLMN). The OCNWDAF uses the *NnF* interface for data collection. The figure below depicts the interface:

Figure 4-1 NnF Interface



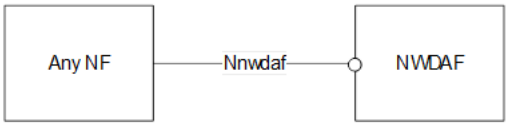
The OCNWDAF uses the *NnF* interface to:

- Request a subscription for data delivery from a particular context.
- Cancel a subscription for data delivery from a particular context.
- Request a specific data report for a particular context.

4.2 Analytics Collection by a Network Function

A 5G NF can request network analytics information from the OCNWDAF through a *Nnwdaf* interface, where the OCNWDAF and the NF belong to the same PLMN. The diagram below depicts the *Nnwdaf* interface:

Figure 4-2 Nnwdaf Interface



The *Nnwdaf* interface is used to:

- Request subscription to network analytics delivery for a particular context.
- Cancel subscription to network analytics delivery for a particular context.
- Request a specific report of network analytics for a particular context.

5
OCNWDAF Services

This chapter describes the OCNWDAF services.

5.1 Analytics Subscription Service

The Analytics Subscription Service handles the subscription and notification functions in the OCNWDAF. The NF service consumers can subscribe or unsubscribe to the notification for different analytics information from the OCNWDAF through this service. The service is implemented as per 3GPP TS 29.520(v16.11).

The consumer NFs use the APIs for subscribing or unsubscribing and updating the existing subscription for OCNWDAF analytics events. The consumers are notified of the observed events as per the subscription request, and the notification can be:

- **A single notification:** Analytics Subscription Service sends only a single notification and purges the subscription.
- **A periodic notification:** Analytics Subscription Service receives the periodic analytics generated from the Analytics Generation Service as per the notification period specified in the subscription request. A notification is generated for the received analytics data. On receiving this notification, subscriptionId and Notification URI mapping is fetched, notification data is prepared, and a REST call is made to the Notification URI.
- **A specific event notification:** The Analytics Subscription Service processes the subscription request, validates the subscription information, generates the subscriptionID, and stores the subscription request in the subscription database. The Data Collection Service waits for the notification data corresponding to the observed events (such as configured thresholds breached) from the Analytics Generation Service and is invoked by using REST APIs.

The subscription can be for descriptive (KPIs and statistics) and predictive analytics (future event prediction). The subscription data is validated, and requests are stored in the subscription database.

Based on the subscription data, the Analytics Subscription Service intimates the Data Collection Service to gather data corresponding to the subscribed events from one or more NF functions.

The probable consumers of the *Nnwdaf_EventsSubscription* service are listed below:

- Policy Control Function (PCF)
- Network Slice Selection Function (NSSF)
- Access and Mobility Management Function (AMF)
- Session Management Function (SMF)
- Network Exposure Function (NEF)
- Application Function (AF)
- Operations, Administration, and Maintenance (OAM)

The Nnwdaf interface is used for communication between the 5G consumers and OCNWDAF in the *Nnwdaf_EventsSubscription* service.

5.2 Analytics Information Service

The Analytics Information Service enables the consumer NFs to request and get specific analytics from the OCNWDAF. The *nwdaf-analyticsinfo* service manages the functions related to the Analytics Information Service. The service is implemented according to 3GPP TS 29.520(v16.0). Analytics Information Service is a REST API based service.

> **Note**
>
> This service handles only HTTP2 requests.

The Analytics Information Service provides the following kinds of analytics information:

- Descriptive Analytics: If the parameters startTime and endTime specify a past time, then the request is for the statistics reports.
- Predictive Analytics: If the parameters startTime and endTime specify a future time, then the request is for the predictive analytics.

The Analytics Information Service provides analytics information corresponding to the Analytics ID in the consumer request.

The probable consumers of the *Nnwdaf_AnalyticsInfo* service are listed below:

- Policy Control Function (PCF)
- Network Slice Selection Function (NSSF)
- Access and Mobility Management Function (AMF)
- Session Management Function (SMF)
- Network Exposure Function (NEF)
- Application Function (AF)
- Operation, Administration, and Maintenance (OAM)

5.3 Data Collection Services

The following OCNWDAF services perform data collection:

- Data Collection Controller service: This service handles the NF instance identification for the UEs and raises subscription requests to various NFs for NF data (if OCNADD is not the assigned data source for the given data collection category). The NF data includes session or location information. It also receives notifications from the NFs for the subscribed events and enables the OCNWDAF to obtain appropriate data with proper granularity.
- Data Collection service: This service collects data and streams data to the CAP4C analytics engine for further processing. It also retrieves behavior data for individual UEs or groups of UEs and global UE information.

Data is collected from the sources listed below for different types of analytics:

- Global management data configured by the service provider.
- NF's data available in the 5G network.

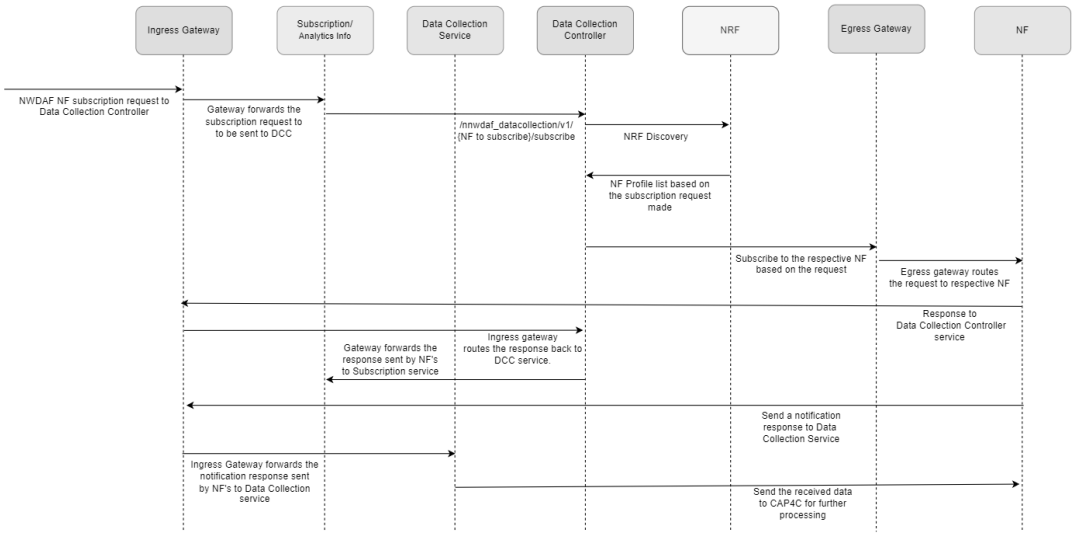
- Data available in the individual NFs (for example, UE or UE group information).
- Oracle Communications Network Analytics Data Director (OCNADD).

The operator can configure the OCNWDAF to collect analytics information from the NFs for upcoming analytics requests. The operator defines the volume and maximum data storage. If the OCNWDAF has collected sufficient data to provide the requested information, it can skip the data collection procedure. The OCNWDAF can send an error response to the analytics consumer if the requested analytics are not available with the OCNWDAF.

Data Collection Workflow

The following workflow depicts the data collection procedure:

Figure 5-1 Data Collection



1. The OCNWDAF invokes an analytics subscription (or analytics information) request to the Data Collection Controller service. The Ingress Gateway service forwards the request to the Data Collection Controller service.
2. The Data Collection Controller sends an NRF Discovery request to the NRF. The NRF responds with an NF profile list based on the subscription request.
3. The Data Collection Controller invokes a subscription request to the required NF from the profile list. The Egress Gateway routes the request to the NF.
4. The NF response is routed back to the Data Collection Controller through the Ingress Gateway. The Ingress Gateway forwards the response to the Analytics Subscription (or Analytics Information) service.
5. The NF sends data collection notification to the Data Collection Service, the notification is routed to the Data Collection Service through the Ingress Gateway.
6. The data received by the Data Collection service is sent to the CAP4C for further processing.

The collected data helps in computing predictive and descriptive analytics based on the AnalyticsID. Following AnalyticsIDs are supported:

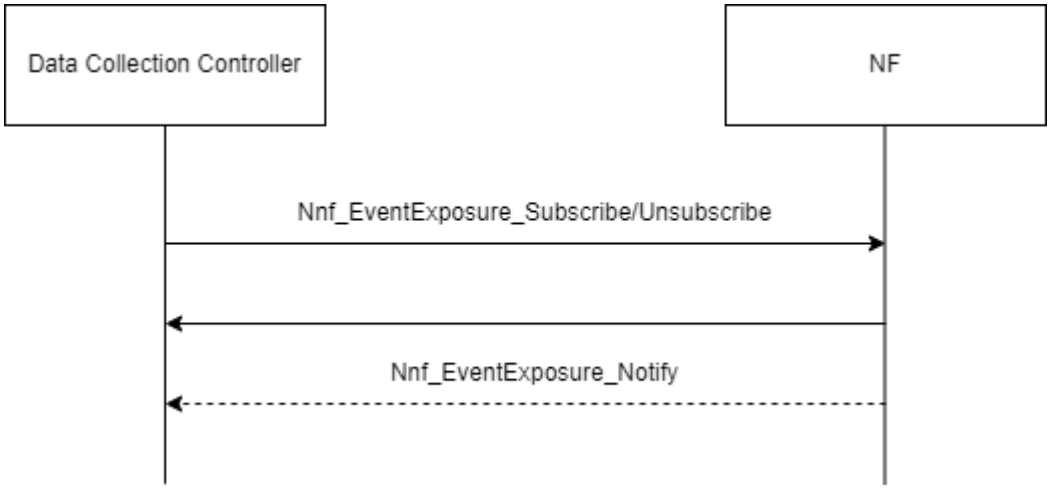
- UE Mobility

- Slice Load Level
- Abnormal behavior (unexpected UE location and Geofence movements)
- NF Load
- Network Performance
- User Data Congestion
- QoS Sustainability

Data Collection from NFs

The following call flow depicts the data collection procedure from various NFs:

Figure 5-2 Data Collection from NFs



1. The Data Collection Controller Service enables the OCNWDAF to subscribe or unsubscribe to an Event ID (or a set of Event ID(s)) by invoking the *Nnf_EventExposure_Subscribe* or *Nnf_EventExposure_Unsubscribe* service operation.
2. The NFs notify the OCNWDAF with requested analytics (for example, event report) by invoking the *Nnf_EventExposure_Notify* service operation.

The following event exposure services enable OCNWDAF data collection:

Table 5-1 Exposure Services

Service producer	Service
AMF	Namf_EventExposure
SMF	Nsmf_EventExposure
UDM	Nudm_EventExposure
NEF	Nnef_EventExposure
NRF	Nnrf_NFDiscovery Nnrf_NFManagement

Data Collection from NRF

The OCNWDAF uses the NRF NF discovery service (*Nnrf_NFDiscovery*) to dynamically discover NF instances and their services in the 5G Core (5GC). This activity can be periodic or

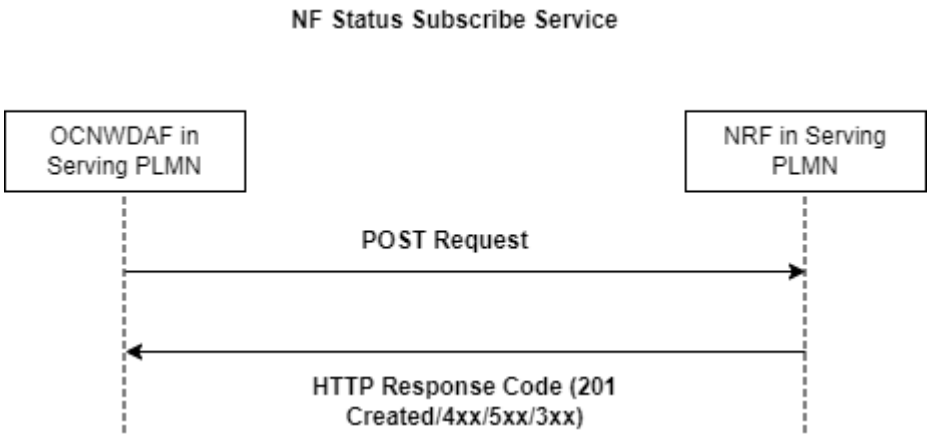
based on any specific event in the network. The OCNWDAF also utilizes the NRF MF Management Service (*Nnrf_NFManagement*), NFStatusSubscribe (*NFStatusSubscribe*), and *NFStatusNotify* services to obtain information about change in NF status. The information collected by these NRF services is used for obtaining NF Load analytics and maintaining a network map for data collection.

> **Note**
>
> The *Nnrf_NFDiscovery* service is invoked only after *NFStatusSubscribe* service to eliminate race conditions of NF status change after the NRF discovery but before the *NRFStatusSubscribe* service.

NRF NFStatusSubscribe Service

The *NFStatusSubscribe* service is used to create an OCNWDAF subscription to the NRF. The OCNWDAF gets notified by the NRF when a specific NF instance profile or set of NF instance profiles are modified or deregistered in the NRF.

Figure 5-3 NF Status Subscribe

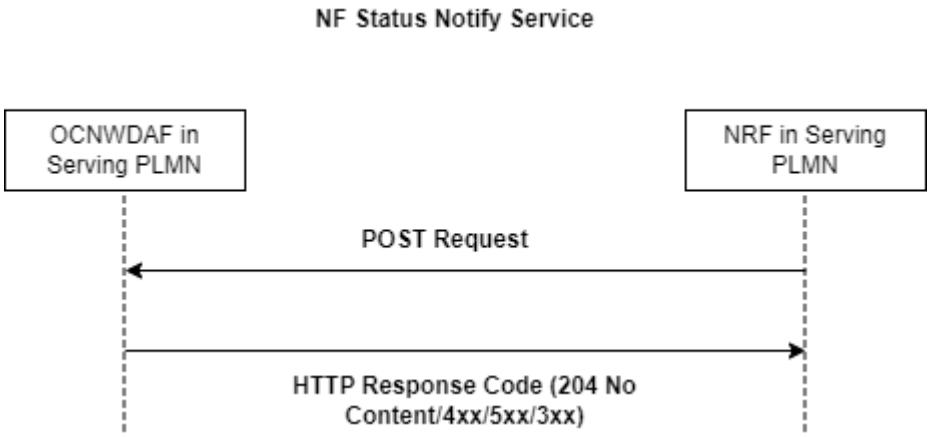


1. The OCNWDAF invokes the *NFStatusSubscribe* service to receive notifications about events (such as registration, deregistration, profile change) related to the Target NF located in the same PLMN by a POST request to the NRF.
2. The NRF authorizes or rejects the subscription request based on the validity of attributes in the POST request.
3. If the request is successful, a subscription is created and a HTTP response code "201 Created" is returned to the OCNWDAF.
4. If the request fails an appropriate HTTP response code is returned (4xx, 5xx or 3xx) indicating the reason for the failure.

NRF NFStatusNotify Service

This service operation notifies the OCNWDAF subscribed to NRF about registration (or deregistration) and profile changes of target NF (or NF instances).

Figure 5-4 NF Status Notify

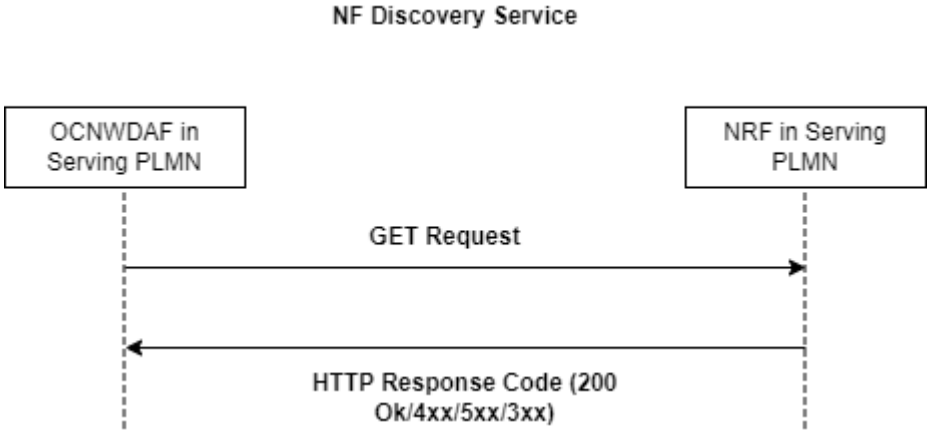


1. The NRF invokes the *NFStatusNotify* service POST request to the subscribed OCNWDAF to indicate any registration or profile changes in the target NF (or NF instances).
2. If the request is successful, the OCNWDAF responds with a "204 No content" HTTP response code.
3. If the request fails an appropriate HTTP response code is returned (4xx, 5xx or 3xx) indicating the reason for the failure.

NRF NFDiscover Service

This service is used to obtain a set of NF instances (represented by their NF profile) that are currently registered with the NRF based on the input query parameters. The results are obtained in the *SearchResult* format. The information obtained is stored for further processing to obtain NF load analytics.

Figure 5-5 NF Discovery Service



1. The OCNWDAF invokes the *NFDiscover* service GET request with query parameter "nf-instances" to the NRF.
2. If the request is successful, the NRF responds with a "200 OK" HTTP code with the response body containing the requested NF profile information based on the request query.

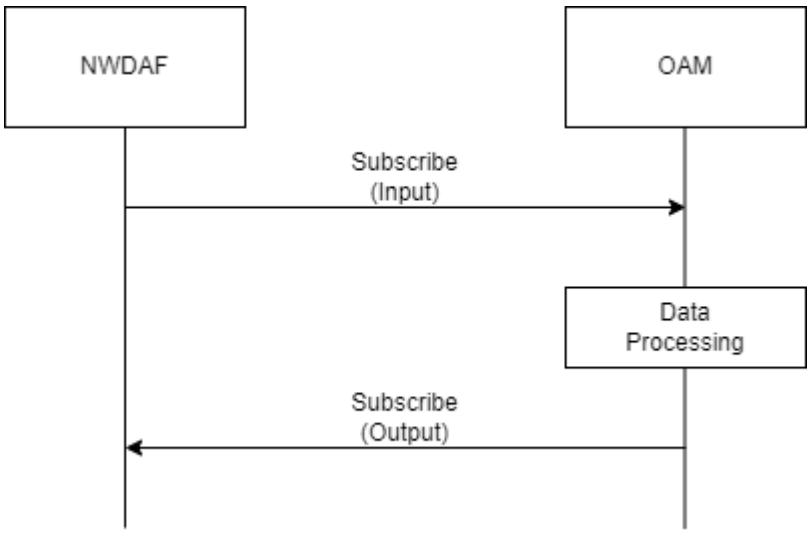
3. If the request fails an appropriate HTTP response code is returned (4xx, 5xx or 3xx) indicating the reason for the failure.

Data Collection from Operations, Administration, and Maintenance (OAM)

The OCNWDAF subscribes to the OAM for the data required to compute analytics information. The OAM processes the request and provides the requested data to the OCNWDAF.

The following call flow depicts the data collection procedure from the OAM:

Figure 5-6 Data Collection from OAM

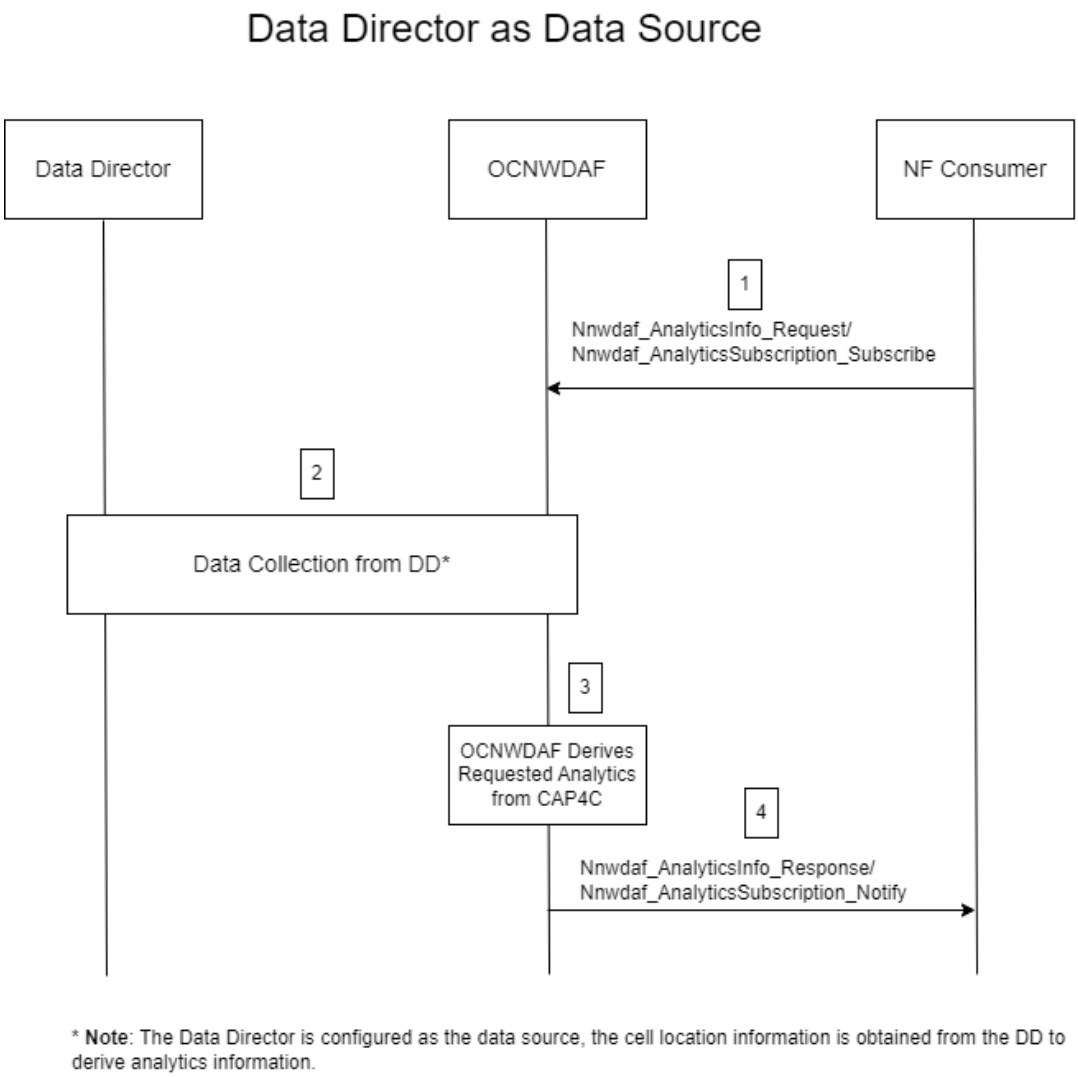


1. OCNWDAF subscribes to the notifications related to the services provided by the OAM.
2. Based on the subscription request from OCNWDAF, the OAM performs data processing and prepares the data to be shared with the OCNWDAF.
3. OCNWDAF obtains the requested data from the OAM.

Data Collection from OCNADD

The Oracle Communications Network Analytics Data Director (OCNADD) can be configured as a data collection source for the OCNWDAF. For more information, see Data Director (OCNADD) Integration.

Figure 5-7 Data Collection from OCNADD



* **Note**: The Data Director is configured as the data source, the cell location information is obtained from the DD to derive analytics information.

1. The analytics consumer sends an analytics request to the OCNWDAF . The analytics request is either an analytics subscription request (*Nnwdaf_AnalyticsSubscription_Subscribe*) or an analytics information request (*Nnwdaf_AnalyticsInfo_Request*).
2. The OCNWDAF collects the required data such as cell location or session information from the OCNADD.
3. The OCNWDAF derives the required analytics from the Analytics Engine CAP4C.
4. The OCNWDAF sends the analytics information to the analytics consumer through a *Nnwdaf_AnalyticsSubscription_Notify* or *Nnwdaf_AnalyticsInfo_Request* message.

The data collected helps in computing analytics based on the AnalyticsID. Listed below are the AnalyticsIDs supported when the data collection source is configured as OCNADD:

- UE Mobility
- Slice Load Level
- Abnormal Behavior (unexpected UE location)

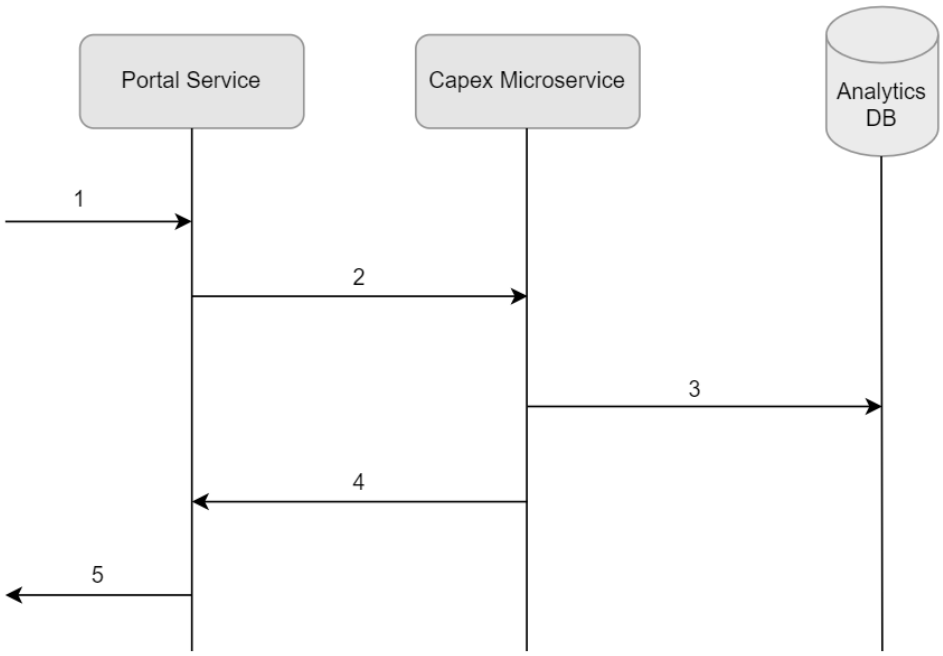
5.4 Capex Optimization Service

The Capex Optimization service interfaces between the Portal Service and the Analytics DB Service to facilitate configuration of Capex Groups and generation of Capex metrics information.

Capex Service

The following diagram displays the workflow adopted for creating Capex groups:

Figure 5-8 Capex Service



1. User raises a request to create a Capex group on the Portal Service (or GUI) by providing information required to create a Capex group.
2. The Portal Service (GUI) requests to the Capex Optimization Microservice to create the group.
3. The Capex Optimization Microservice processes this data and stores it in the Analytics DB.
4. The Capex group is successfully created and the Capex Microservice sends a success message to the Portal Service (GUI).
5. The Portal Service (GUI) displays the newly created Capex group and the corresponding analytics for that Capex group.

To view Network Performance and User Data Congestion Prediction per Capex Group, see Machine Learning (ML) Model Selector.

To access the Capex Optimization page, create Capex groups and view Capex Metrics on the OCNWDAF GUI, see Capex Optimization.

6

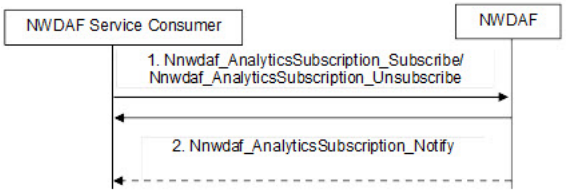
OCNWDAF Subscription and Analytics Requests

This chapter describes consumer subscription and analytics request procedures.

6.1 Analytics Subscription Request to the OCNWDAF

This section describes how the OCNWDAF service consumers subscribe or unsubscribe to the OCNWDAF to obtain analytics information. The *Nnwdaf_AnalyticsSubscription* service is used to subscribe, unsubscribe, and modify existing subscriptions to the OCNWDAF.

Figure 6-1 OCNWDAF Consumer Subscription Request

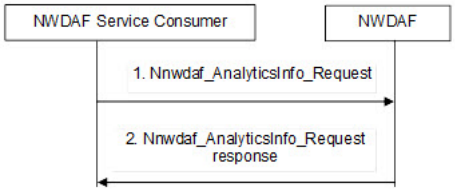


1. The OCNWDAF service consumer initiates or cancels a subscription to analytics information by invoking the *Nnwdaf_AnalyticsSubscription_Subscribe* or *Nnwdaf_AnalyticsSubscription_Unsubscribe* service operation. When a subscription to analytics information is received, the OCNWDAF determines whether triggering data collection is required. If the service invocation is for a subscription modification, the NF service consumer includes an identifier (Subscription Correlation ID) to be modified in the *Nnwdaf_AnalyticsSubscription_Subscribe* request.
2. If the OCNWDAF service consumer subscribes to analytics information, the OCNWDAF notifies the service consumer with the analytics information by invoking the *Nnwdaf_AnalyticsSubscription_Notify* service operation, based on the request from the service consumer, for example, Analytics Reporting Parameters.

6.2 Analytics Information Request to OCNWDAF

This section describes how the OCNWDAF service consumers request and obtain analytics information from the OCNWDAF. The *Nnwdaf_AnalyticsInfo* service is used to request and obtain information from the OCNWDAF.

Figure 6-2 Analytics Request



1. The OCNWDAF service consumer requests analytics information by invoking the *Nnwdaf_AnalyticsInfo_Request* service operation.
2. On receiving the request, the OCNWDAF determines if a data collection needs to be triggered. If the requested analytics information is not present, it triggers a data collection request.
3. If the OCNWDAF has the requested information, it responds to the consumer with the requested analytics information.

> **Note**
>
> The consumer sends an HTTP GET request to obtain analytics data based on the query parameter value of the "*event-id*" attribute. Along with *event-id*, the *ana-req* attribute can be specified. It contains the parameter *timeAnaNeeded*, which sets the time when the analytics information is needed. Once the time specified *timeAnaNeeded* is crossed, the consumer does not need to wait for the analytics information any longer, and the OC-NWDAF sends an error response to the consumer.

6.3 Correlation between Network Data and Service Data

The correlation information from each NF input data helps OCNWDAF correlate data from different NFs. The following table contains correlation information:

> **Note**
>
> The correlation information is not listed in the input data per network data analytics.

Table 6-1 Correlation between network data and service data

Correlation Information	Description
Timestamp, IP address 5-tuple	To correlate data from AF and from UPF
Timestamp, AN Tunnel Info (Clause 9.3.2.2, 3GPP TS 38.413 [16])	To correlate UPF data and OAM data which are reported by the RAN
Timestamp, UE IP address	To correlate data from UPF and SMF
Timestamp, SUPI	To correlate data from SMF and AMF
Timestamp, SUPI, DNN, S-NSSAI or UE IP address	To correlate data from SMF and PCF

Table 6-1 (Cont.) Correlation between network data and service data

Correlation Information	Description
Timestamp, RAN UE NGAP ID (Clause 9.3.3.2, 3GPP TS 38.413 [16]) and Global RAN Node ID	To correlate AMF data and OAM data reported by the RAN
Timestamp, Application ID, IP filter information	To correlate data from SMF and AF

7 OCNWDAF Analytics

The OCNWDAF assists in collecting and analysing data in a 5G network. An OCNWDAF consumer can avail analytics information or reports for various events in the network. The OCNWDAF allows the Communications Service providers (CSPs) to efficiently monitor, manage, automate, and optimise their network operations by analysing the data collected across the network.

The consumers can subscribe (or unsubscribe) to the OCNWDAF to obtain specific analytics reports as a one-time event or periodically get notified when a defined event is detected. The analytics information provided by the OCNWDAF is either statistical information on past events or predictive information which can be used to balance the resources in the network. The OCNWDAF currently supports NFs as data producers but the data consumers can be not only be 5G NFs but AFs and OAM can also be consumers of analytics information.

Listed below are the type of analytics reports that OCNWDAF can provide:

- Historical analytics
- Future analytics
- Reports when a thresholds are crossed

The Analytics Subscription Service and Analytics Information Service are used for obtaining different analytics reports. The Analytics Subscription Service obtains periodic reports based on future or current events, threshold and abnormal event reports. The Analytics Information Service obtains historic statistical reports and prediction reports.

Analytics Request

A consumer analytics request (subscription or information request) to the OCNWDAF contains the following information:

- Analytics ID(s): Analytics ID identifies the requested type of analytics.
- Analytics Filter Information (optional)
- Target of Analytics Reporting: The target indicates the object(s) for which Analytics information is requested. It includes entities such as a specific UE or a group of UE(s) or all UEs.
- Analytics Reporting Information with the following parameters:
  - In the case of Analytics Subscription requests, event reporting parameters are defined as per 3GPP TS 29.520.
  - In the case of Analytics Subscription requests, Reporting Thresholds are defined, which are the conditions on the level of each requested analytics. When the threshold is crossed, the OCNWDAF notifies the consumer. The specified conditions may include rules like "ASCENDING", "DESCENDING", or "CROSSED". The default rule is "CROSSED" if no matching rule is provided.
- Analytics target period: Time interval which includes both start and end time (in UTC format). The target period specified can be either the past time or future time.
  - Analytics target period specified in past time indicates an analytics statistics request.

  - Analytics target period specified in the future time indicates an analytics prediction request.

  By setting start time and end time to the same value, the consumer of the analytics can request analytics or subscribe to analytics for a specific time rather than for a time interval.
- Preferred level of accuracy of the analytics (for example, low or high).
- For Analytics Information requests, the time when analytics information is required can be specified. If the time is reached and no analytics are received the consumer does not wait for the analytics information any longer and the OCNWDAF sends an error response to the consumer.
- The maximum number of objects (optional). This specifies the number of objects in a list of analytics for each request.
- Maximum number of SUPIs is an optional parameter that specifies the number of relevant SUPIs in the analytics object to be returned in the analytics response. When this parameter is not specified, the OCNWDAF returns the stipulated number of relevant SUPIs in the analytics object.

Analytics Report

The OCNWDAF provides the following analytics information to the consumer:

- Analytics information based on specified Analytics ID and target time.
- Notification Correlation Information for Analytics Subscription requests.
- The OCNWDAF provides the following additional information:
  - Timestamp of analytics generation. The analytics consumer can determine the relevance of analytics information based on the timestamp received.
  - Validity period, the time until which the analytics information is valid.
  - Probability assertion: This indicates confidence in the prediction. The confidence is expressed as a value based on definition of parameters "Preferred level of accuracy" and "Analytics Target Period" in the consumer request and the data availability with OCNWDAF. The OCNWDAF returns a value of zero confidence if sufficient data is not collected to match the requested accuracy level within the analytics target time. If the analytics target time is not specified, the OCNWDAF waits till adequate data is collected then provides a response or notification.

> **Note**
>
> Statistical analytics does not contain this parameter as confidence in prediction is not applicable for this type of analytics.

The OCNWDAF provides the following analytics:

- Slice Load level analytics
- UE Mobility analytics
- UE Abnormal Behaviour analytics (Unexpected UE Location)
- NF Load Level analytics
- Network Performance analytics
- User Data Congestion analytics (only statistical analytics)
- QoS Sustainability analytics

- Capex Optimization analytics

7.1 QoS (Quality of Service) Sustainability Analytics

Overview

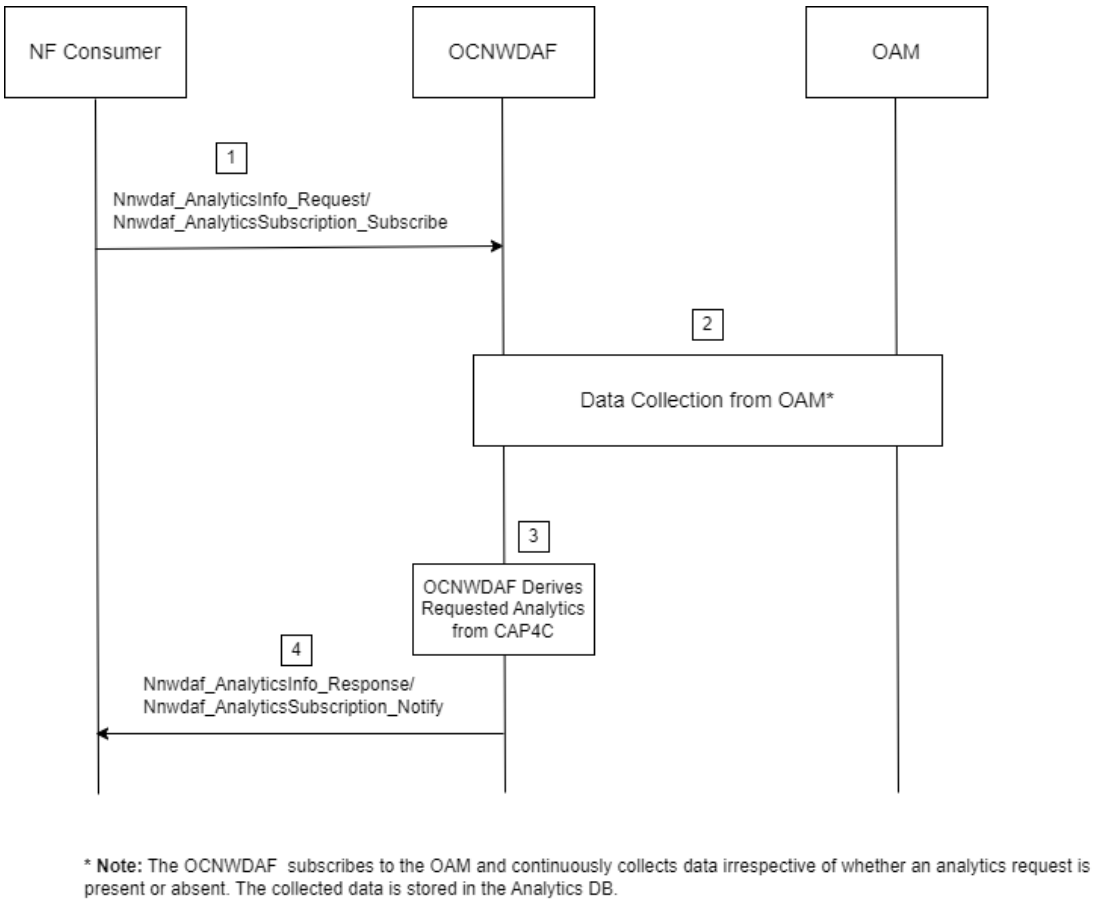
Consumers can derive QoS (Quality of Service) Sustainability Analytics from the OCNWDAF. This analytics information includes QoS change statistics in a target area (for a specified period). OCNWDAF provides both statistical and predictive analytics. Predictive analytics includes information about anticipated QoS changes at a future time in a target area. Consumers can obtain analytics information for a slice by specifying the S-NSSAI of the slice in the analytics request. Users can subscribe for a one-time analytics report or opt for continuous analytics reports from the OCNWDAF.

> **Note**
>
> QoS Analytics subscribers must include the *QoSSustainability* flag in their subscriptions and analytics requests.

QoS Sustainability Analytics Workflow

The following diagram depicts the QoS Sustainability Analytics workflow:

Figure 7-1 QoS Sustainability Analytics Workflow



* **Note:** The OCNWDAF subscribes to the OAM and continuously collects data irrespective of whether an analytics request is present or absent. The collected data is stored in the Analytics DB.

The following procedure describes the workflow:

1. The NF consumer requests (*Nnwdaf_Analyticsinfo_request*) or subscribes to (*Nnwdaf_AnalyticsSubscription_Subscribe*) the OCNWDAF for QoS sustainability analytics information.
2. The OCNWDAF collects the required data from Operation, Administration, and Maintenance (OAM).The OCNWDAF subscribes to the OAM and continuously collects data from it (irrespective of an analytics request being present or absent). This data is stored in the Analytics DB.
3. The OCNWDAF derives the requested analytics from the CAP4C based on the conditions specified in the consumer request.
4. The OCNWDAF provides the QoS sustainability analytics to the consumer NF.

Consumer Request to OCNWDAF

A consumer request for QoS sustainability analytics contains the following information:

- Analytics ID set to "QoS Sustainability”
- Target of Analytics Reporting set to “any UE”
- The following analytics filter information:
  - QoS requirements (mandatory): Either "5QI (5G QoS Identifier)" or "QoS Resource Type."
    - 5QI: For standardized or preconfigured characteristics specified in 3GPP TS 23.501 (table 5.7.4-1), including Packet Delay Budget (PDB) and Packet Error Rate (PER) values.
  - Location information (mandatory): Specified as AoI (Area of Interest,that is, a list of Tracking Areas (TAs) or cells) or a path of interest.
  - S-NSSAI (optional)
- The analytics target period that indicates the time over which the statistics are requested.
- A reporting threshold (optional, and applicable only for analytics subscriptions). A matching direction can be provided along with the reporting threshold such as crossed, below, or above the default value.
- A subscription request also contains the Notification Correlation ID and the Notification Target Address.

Data Collection from OAM

The OCNWDAF collects data the following data from the OAM to generate QoS sustainability analytics:

Table 7-1 Data Collection from OAM

Information	Source	Description
RAN UE Throughput	OAM (3GPP TS 28.554 [10])	Average UE bitrate in the cell (for transfers restricted by the air interface the payload data volume on RLC level per elapsed time unit on the air interface), per timeslot, per cell, per 5QI, and per S-NSSAI.

Table 7-1 (Cont.) Data Collection from OAM

Information	Source	Description
QoS Flow Retainability	OAM (3GPP TS 28.554 [10])	Number of abnormally released QoS flows during the time the QoS Flows were used per timeslot, per cell, per 5QI, and per S-NSSAI.

> **Note**
>
> For a complete list of request parameters, see QoS Sustainability Analytics APIs.

> **Note**
>
> The data types supported by OCNWDAF comply with the 3GPP specifications. For more information about the 3GPP data types, see 3GPP Technical Specification 29.520, Release 17, Network Data Analytics Services.

7.2 User Data Congestion Analytics

Overview

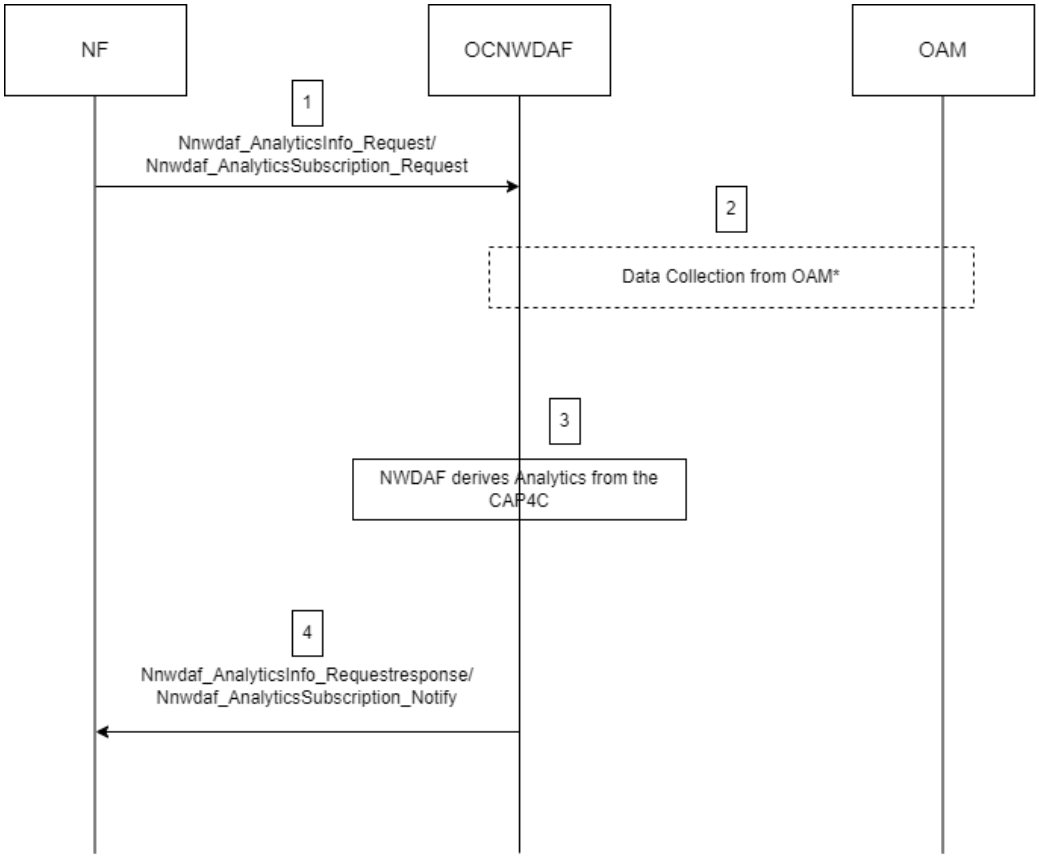
The OCNWDAF provides User Data Congestion Analytics (statistical and threshold) to consumers. It includes information about the congestion experienced during user data transfer over the user plane. The congestion information reported is specific to an Area of Interest (AoI) or an User Equipment (UE). If the consumer provides only the UEs ID, the OCNWDAF determines the AoI in which congestion analytics is required based on the ID. The OCNWDAF also provides congestion analytics for a slice based on the Single-Network Slice Selection Assistance Information (S-NSSAI). User can specify a threshold for the congestion level and the OCNWDAF reports congestion analytics when the threshold is breached. User can subscribe for one-time or continuous analytics reporting. Predictive analytics is not supported.

User Data Congestion Analytics Workflow

User can retrieve analytics information for a specific location or a UE.

The following diagram depicts how User Data Congestion analytics is retrieved:

Figure 7-2 User Data Congestion Analytics Workflow



* **Note:** The OCNWDAF subscribes to the OAM and continuously collects data irrespective of whether an analytics request is present or absent. The collected data is stored in the Analytics DB.

The following procedure describes the workflow:

1. The NF consumer requests (*Nnwdaf_Analyticsinfo_Request*) or subscribes to (*Nnwdaf_AnalyticsSubscription_Request*) the OCNWDAF for User Data Congestion analytics information.
2. The OCNWDAF collects the required data from Operation, Administration, and Maintenance (OAM).The OCNWDAF subscribes to the OAM and continuously collects data from it (irrespective of an analytics request being present or absent). The collected data is stored in the Analytics DB.
3. The OCNWDAF derives the requested analytics from the CAP4C based on the conditions specified in the consumer request.
4. The OCNWDAF provides the User Data Congestion sustainability analytics to the consumer NF. (*Nnwdaf_Analyticsinfo_Requestreponse* or *Nnwdaf_AnalyticsSubscription_Notify*)

Consumer Request to OCNWDAF

A consumer request for user data congestion analytics contains the following information:

- Analytics ID set to "User Data Congestion".

- Target of Analytics Reporting containing single UE (SUPI) or "any UE".
- Analytics Filter Information containing:
  - Traffic type: The allowed options for "Traffic type" are Overall, GBR, or delay-critical GBR. This parameter is mandatory if the target is "any UE". For all other types of "Target of Analytics Reporting", this is an optional parameter.
  - Area of Interest: It consists of a list of Tracking Areas (TAs) or Cells. This is a mandatory parameter if the "Target of Analytics Reporting" is set to "any UE". For all other types of "Target of Analytics Reporting", this is an optional parameter.
  - Optional list of analytics subsets: This includes Area subset (a specific TA or cell ID within the AoI) and Analytics target period.
  - The S-NSSAI to obtain congestion analytics in a network slice. This is an optional parameter.
- Reporting Threshold (optional and applicable only for Analytics Subscriptions).
- Analytics target period indicates the time period over which the statistics are requested.
- The Notification Correlation ID and Notification Target Address are included in an analytics subscription.

Data Collection for User Data Congestion Analytics

The OCNWDAF collects data from AMF, OAM, UPF, and AF to generate user data congestion analytics.

Table 7-2 Data Collection from NF and OAM

Information Collected	Source	Description
UE Location	AMF	The UE location information that OCNWDAF uses to determine the Area of Interest.
Measurements	OAM	Performance Measurements that the OCNWDAF uses to determine congestion levels. Performance Measurements are related to information transfer over the user plane.
Throughput UL/DL	OAM	Average throughput Uplink (UL)/ (Downlink) DL over the measurement period.
Throughput UL/DL (peak)	OAM	Peak throughput UL/DL over the measurement period.

Request/Response Parameters

Listed below are the parameters in the user data congestion analytics both in request and response:

Table 7-3 Request Parameters

Parameter	Data Type	Presence	Description
eventSubscriptions	array(EventSubscription)	M	Specifies the subscribed event. The event parameter within the subscription is set to "USER DATA CONGESTION".
evtReq	ReportingInformation	O	Represents the reporting requirements of the event subscription. If this parameter is not provided, the default values for *ReportingInformation* is used. The notification method "notifMethod" within *ReportingInformation* takes precedence over the *notificationMethod* within *EventSubscription*.
notificationURI	Uri	C	The URI to which OCNWDAF sends the reports
eventNotifications	array(EventNotification)	C	Notifications about individual events This parameter is present if the immediate reporting indication in the "*immRep*" attribute within the "*evtReq*" attribute is set to true in the event subscription and the reports are available. This parameter is provided in response to the OCNWDAF subscription if *immediatereport* is true and the reports are available.

Table 7-3 (Cont.) Request Parameters

Parameter	Data Type	Presence	Description
failEventReports	array(FailureEventInfo)	O	This parameter is provided by the OCNWDAF. When this parameter is available, it contains the event(s) for which the subscription is not successful, it also includes the failure reason(s). This parameter is populated and returned in the response for the error case.
consNfInfo	ConsumerNfInformation	O	Represents the analytics consumer NF information
notifCorrId	String	M	Notification correlation identifier. It is generated after a successful subscription and is returned in the response.
supportedFeatures	SupportedFeatures	C	This parameter is provided by the NF service consumer in the POST request for creating an OCNWDAF Event Subscription resource, and it is also provided in response to the corresponding request.

> **Note**
>
> For a complete list of request parameters, see User Data Congestion Analytics APIs.

> **Note**
>
> The data types supported by OCNWDAF comply with the 3GPP specifications. For more information about the 3GPP data types, see 3GPP Technical Specification 29.520, Release 17, Network Data Analytics Services.

Output User Data Congestion Analytics

The following analytics information is obtained:

- User Data Congestion Statistics

Table 7-4 User Data Congestion Analytics

Parameter	Data Type	Presence	Description
event	NwdafEvent	M	Event that is notified.
start	DateTime	O	UTC time indicating the start time of the observation period. The absence of this attribute means subscription at present time.
expiry	DateTime	O	It defines the expiration time after which the analytics information becomes invalid.
timeStampGen	DateTime	O	It defines the timestamp of analytics generation.
userDataCongInfos	array	C	The user data congestion information.

UserDataCongestionInfo

Table 7-5 UserDataCongestionInfo

Attribute Name	Data Type	P	Description
networkArea	NetworkAreaInfo	M	The network area to which the subscription applies.
congestionInfo	CongestionInfo	M	The congestion information of the specific location.
snssai	Snssai	C	Identifies an S-NSSAI. Is present if the "snssais" was provided within the EventSubscription during the subscription for event notification procedure.

Type CongestionInfo

Table 7-6 CongestionInfo

Attribute Name	Data type	P	Description
congType	CongestionType	M	Identifies the congestion analytics type.
timeIntev	TimeWindow	M	Represents a start time and a stop time requested for the congestion information.
nsi	ThresholdLevel	M	Network status indication.

Table 7-6 (Cont.) CongestionInfo

Attribute Name	Data type	P	Description
congestionDirection	String	M	Identifies if the report being generated is for Uplink or Downlink congestion.

Enumeration CongestionType

Table 7-7 CongestionType

Enumeration Value	Description
USER_PLANE	The congestion analytics type is user plane.

> **Note**
>
> The data types supported by OCNWDAF comply with the 3GPP specifications. For more information about the 3GPP data types, see 3GPP Technical Specification 29.520, Release 17, Network Data Analytics Services.

7.3 Network Performance Analytics

Overview

The OCNWDAF provides network performance analytics to the consumer. It includes information about resource consumption by the gNodeB (gNB), a key component in the 5G Radio Access Network (RAN), as well as key mobility performance indicators in the Area of Interest (AoI). The gNodeB is a base station in the 5G network. The network performance analytics provides information such as gNB status, gNB resource usage, communication, and mobility performance in the Area of Interest (AoI). It also provides statistics or predictions on the number of UEs in that AoI. The OCNWDAF can provide predictive or statistical analytics based on consumer requests.

The OCNWDAF GUI is enhanced to display the following information:

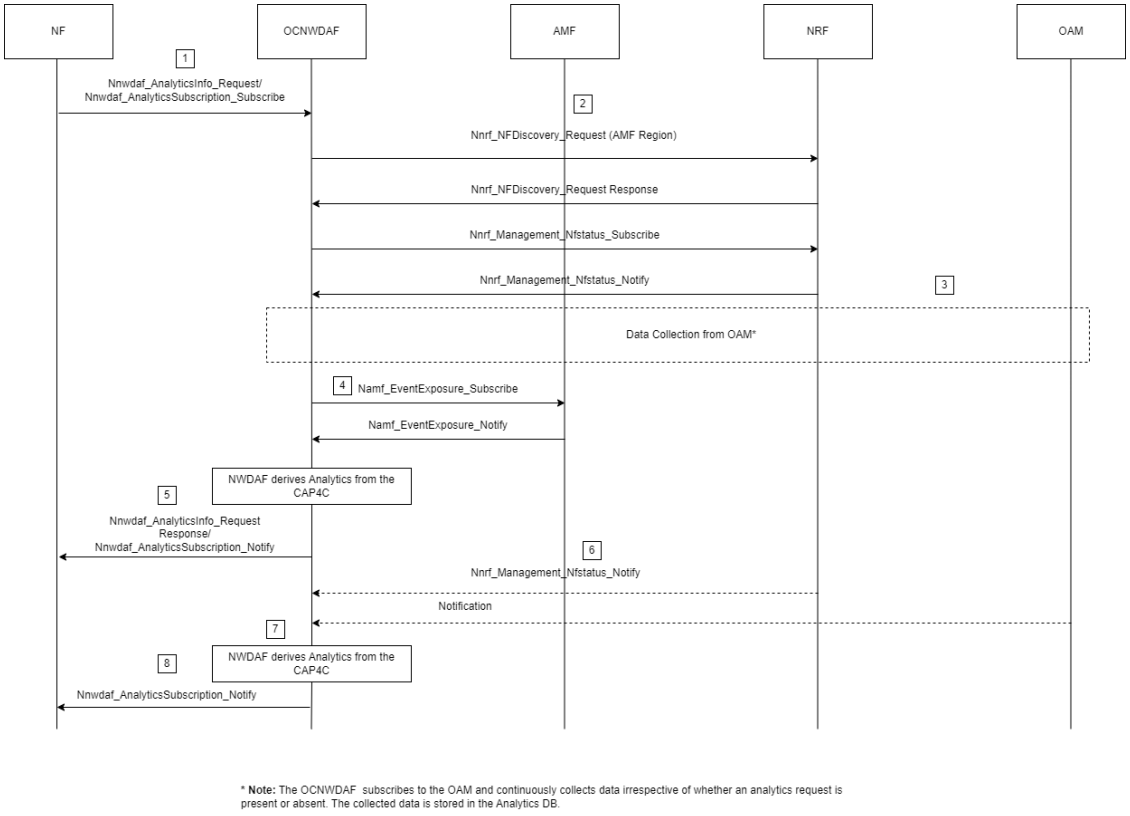
- All available cells in a selected Tracking Area
- For each cell, the user can view the following information:
  - GNB Computing, Memory, and Disk Usage
  - Session Success Ratio
  - Hand Over (HO) Success Ratio
- The user can set a threshold value, select a tracking area and a time interval in the GUI. All the available cells in the selected tracking area within the selected time interval and specified threshold value are displayed on the screen.

For more information, see Monitoring page on the OCNWDAF GUI.

Network Performance Analytics Workflow

The following diagram depicts the workflow of an analytics consumer request to OCNWDAF for Network Performance analytics:

Figure 7-3 Network Performance Analytics Workflow



* **Note:** The OCNWDAF subscribes to the OAM and continuously collects data irrespective of whether an analytics request is present or absent. The collected data is stored in the Analytics DB.

1. The analytics consumer sends an analytics request to the OCNWDAF for Network Performance analytics. The analytics request is either an analytics subscription request *(Nnwdaf_AnalyticsSubscription_Subscribe)* or an analytics information request *(Nnwdaf_AnalyticsInfo_Request)*. In the request, the Analytics ID is set to *Network Performance*. The request also specifies the target of analytics reporting, the filter (*Area of Interest*), reporting thresholds, and the analytics target period.
2. The OCNWDAF sends a discovery request to the NRF to obtain information about the AMFs present in the AMF region of the Area of Interest (AoI). The OCNWDAF subscribes to the NRF to get the NF load and status information about these AMFs.
3. The OCNWDAF subscribes to the OAM and continuously collects data irrespective of whether an analytics request is present or absent. The collected data is stored in the Analytics DB.
4. The OCNWDAF collects information about the number of UEs in the Area of Interest from the AMF using *Namf_EventExposure_Subscribe* service and the Target of Event Reporting specified in the analytics request.
5. The OCNWDAF derives the analytics information from the CAP4C and sends either a *Nnwdaf_AnalyticsSubscription_Notify* or *Nnwdaf_AnalyticsInfo_Request response* to the analytics consumer.

6. The OCNWDAF is notified about any change in the network performance, such as a change in gNB status, gNB resource usage, communication, and mobility performance in the AoI during the specified target period. The OAM detects the changes or changes in the NF load is reported by the NRF.
7. The OCNWDAF derives analytics from CAP4C based on the most recently collected data.
8. The OCNWDAF uses the *Nnwdaf_AnalyticsSubscription_Notify* to notify the analytics consumer about changes in the analytics information during the specified analytics target period or when reporting thresholds are breached.

Consumer Request to OCNWDAF

A consumer request for Network Performance analytics contains the following information:

- The analytics ID is set to *Network Performance*.
- The Target of Analytics Reporting: This can be a UE or internal group identifier of a group for which the analytics information is required. The group contains the UEs that are located in the Area of Interest during the time specified in the Analytics target period. The target of analytics reporting is set to *"any UE"* by default.
- Analytics filter information consisting of the following:
  - Area of Interest (a list of TA or Cells) specifying the focus area. This parameter is mandatory if the Target of Analytics Reporting parameter is set to "any UE". Providing the filter information is optional if the Target of Analytics Reporting parameter is set to any other value.
  - Subset of analytics (optional)
- Reporting threshold (optional)
- Analytics target period, the period for which the statistics or predictions are required.
- Maximum number of objects (optional)
- In an analytics subscription request, the Notification Correlation Id and the Notification Target Address are included.

Request/Response Parameters

Listed below are the parameters in the network performance analytics request and response:

Table 7-8 Request/Response Parameters

Parameter	Data Type	Presence	Description
eventSubscriptions	array(EventSubscription)	M	Specifies the subscribed event. The event parameter within the subscription is set to "NETWORK_ PERFORMANCE".

Table 7-8 (Cont.) Request/Response Parameters

Parameter	Data Type	Presence	Description
evtReq	ReportingInformation	O	Represents the reporting requirements of the event subscription. If this parameter is not provided, the default values for *ReportingInformation* is used. The notification method "notifMethod" within *ReportingInformation* takes precedence over the *notificationMethod* within *EventSubscription*.
notificationURI	Uri	C	The URI to which OCNWDAF sends the reports.
eventNotifications	array(EventNotification)	C	Notifications about individual events. This parameter is present if the immediate reporting indication in the "*immRep*" attribute within the "*evtReq*" attribute is set to true in the event subscription and the reports are available. This parameter is provided in response to the OCNWDAF subscription if *immediatereport* is true and the reports are available.
failEventReports	array(FailureEventInfo)	O	This parameter is provided by theOCNWDAF. When this parameter is available, it contains the event(s) for which the subscription is not successful, it also includes the failure reason(s). This parameter is populated and returned in the response for the error case.
consNfInfo	ConsumerNfInformation	O	Represents the analytics consumer NF information.

Table 7-8 (Cont.) Request/Response Parameters

Parameter	Data Type	Presence	Description
notifCorrId	String	M	Notification correlation identifier. It is generated after a successful subscription and is returned in the response.
supportedFeatures	SupportedFeatures	C	This parameter is provided by the NF service consumer in the POST request for creating an OCNWDAF Event Subscription resource, and it is also provided in response to the corresponding request.

Note

- For a complete list of request parameters see, Network Performance Analytics APIs.
- The data types supported by OCNWDAF comply with the 3GPP specifications. For more information about the 3GPP data types, see *3GPP Technical Specification 29.520, Release 17, Network Data Analytics Services*.

Network Performance Data Collection

The OCNWDAF requires resource utilization and RAN status of the gNbs to generate Network Performance analytics. It also requires PDU session and UE Handover information. This information is obtained from OAM. The Network Performance ID also requires information on the number of UEs from the AMF. The OCNWDAF collects the needed information from the following sources to generate Network Performance analytics:

Table 7-9 Data Collection

Information Collected	Source	Description
gNodeB Resource Utilization (CPU, Memory, Storage)	OAM	Radio resource utilization information.
RAN Status	OAM	The status of the RAN.
PDU Session Success and Failure	OAM	Success or failure information of PDU sessions.
UE Handover Success and Failure	OAM	Success or failure information of UE handovers.
Number of UEs	AMF	Number of UEs in Area Report.

For more information see, Data Collection Services

Output Network Performance Analytics

The following types of analytics information is obtained:

- Network Performance statistics
- Network Performance predictions

The predictive analysis has an additional parameter, "Confidence", which indicates the accuracy of the prediction.

Table 7-10 Network Performance Analytics

Parameter	Data Type	Presence	Description
event	NwdafEvent	M	Event that is notified.
start	DateTime	O	UTC time indicating the start time of the observation period. The absence of this attribute means subscription at present time.
expiry	DateTime	O	It defines the expiration time after which the analytics information becomes invalid.
timeStampGen	DateTime	O	It defines the timestamp of analytics generation.
duration	Duration	C	It defines the time period for which the threshold was in the target state.
nwPerfs	array (NetworkPer fInfo)	C	The network performance information.

Type NetworkPerfInfo

Table 7-11 NetworkPerfInfo

Attribute Name	Data type	P	Description
networkArea	NetworkAreaInfo	M	The network area to which the subscription applies.
nwPerfType	NetworkPerfType	M	The type of network performance.
relativeRatio	SamplingRatio	O	The reported relative ratio expressed in percentage. Either the relativeRatio or absoluteNum is provided.
absoluteNum	Uinteger	O	The reported absolute number.

Table 7-11 (Cont.) NetworkPerfInfo

Attribute Name	Data type	P	Description
confidence	Uinteger	C	Indicates the confidence of the prediction. If sufficient data is unavailable during the specified analytics target time interval, the confidence value returned is "0".

Type NetworkAreaInfo

Table 7-12 NetworkAreaInfo

Attribute name	Data type	P	Cardinality	Description
ecgis	Array	O	0 to N	Is the list of E-UTRA cell identities.
ncgis	Array	O	0 to N	Is the list of NR cell identities
gRanNodeIds	Array	O	0 to N	Is the list of list of the NG-RAN nodes.
tais	Array	O	0 to N	Is the list of tracking area identities.

Enumeration NetworkPerfType

Table 7-13 NetworkPerfType

Enumeration value	Description
GNB_ACTIVE_RATIO	Indicates the ratio of active gNBs (up and running) to the total number of gNBs.
GNB_COMPUTING_USAGE	Indicates the gNodeBs computing resource usage.
GNB_MEMORY_USAGE	Indicates gNodeBs memory usage.
GNB_DISK_USAGE	Indicates gNodeBs disk usage.
NUM_OF_UE	Indicates the number of UEs.
SESS_SUCC_RATIO	Indicates the ratio of the successful PDU session setups to the total PDU session setup attempts.
HO_SUCC_RATIO	Indicates the ratio of successful handovers to the total handover attempts.

The analytics report consists of the following information:

Table 7-14 Analytics Report

Information	Description
Area subset	TA or Cell ID within the requested area of interest .

Table 7-14 (Cont.) Analytics Report

Information	Description
Analytics target period subset	Defined time window within the requested analytics target period.
gNB status information	Average ratio of gNBs that are up and running during the entire analytics target period in the area subset.
gNB resource usage	Average usage of assigned resources.
gNB resource usage for GBR traffic	Average usage of assigned resources (average, peak).
gNB resource usage for Delay-critical GBR traffic	Average usage of assigned resources (average, peak).
Number of UEs	Average number of UEs observed in the area subset.
Communication performance	Average ratio of successful PDU sessions setup.
Mobility performance	Average ratio of successful handovers.
Confidence (only for predictions)	Percentage accuracy of prediction.

> **Note**
>
> The data types supported by OCNWDAF comply with the 3GPP specifications. For more information about the 3GPP data types, see *3GPP Technical Specification 29.520, Release 17, Network Data Analytics Services*.

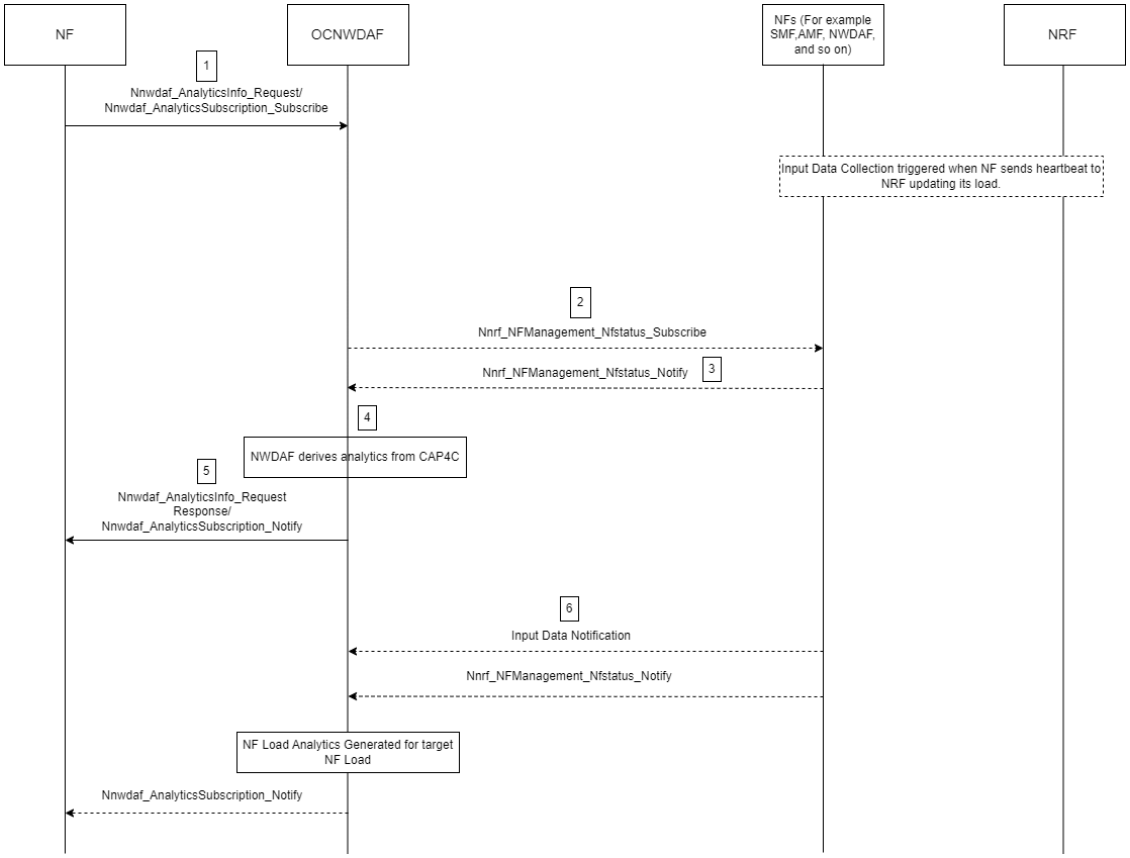
7.4 Network Function (NF) Load Analytics

The OCNWDAF can provide NF load analytics information to the analytics consumer. The analytics generated by OCNWDAF can be either predictive or statistical, based on the type of consumer analytics request.

NF Load Analytics Workflow

The following workflow depicts an analytics consumer request to OCNWDAF for NF load analytics:

Figure 7-4 NF Load Analytics Workflow

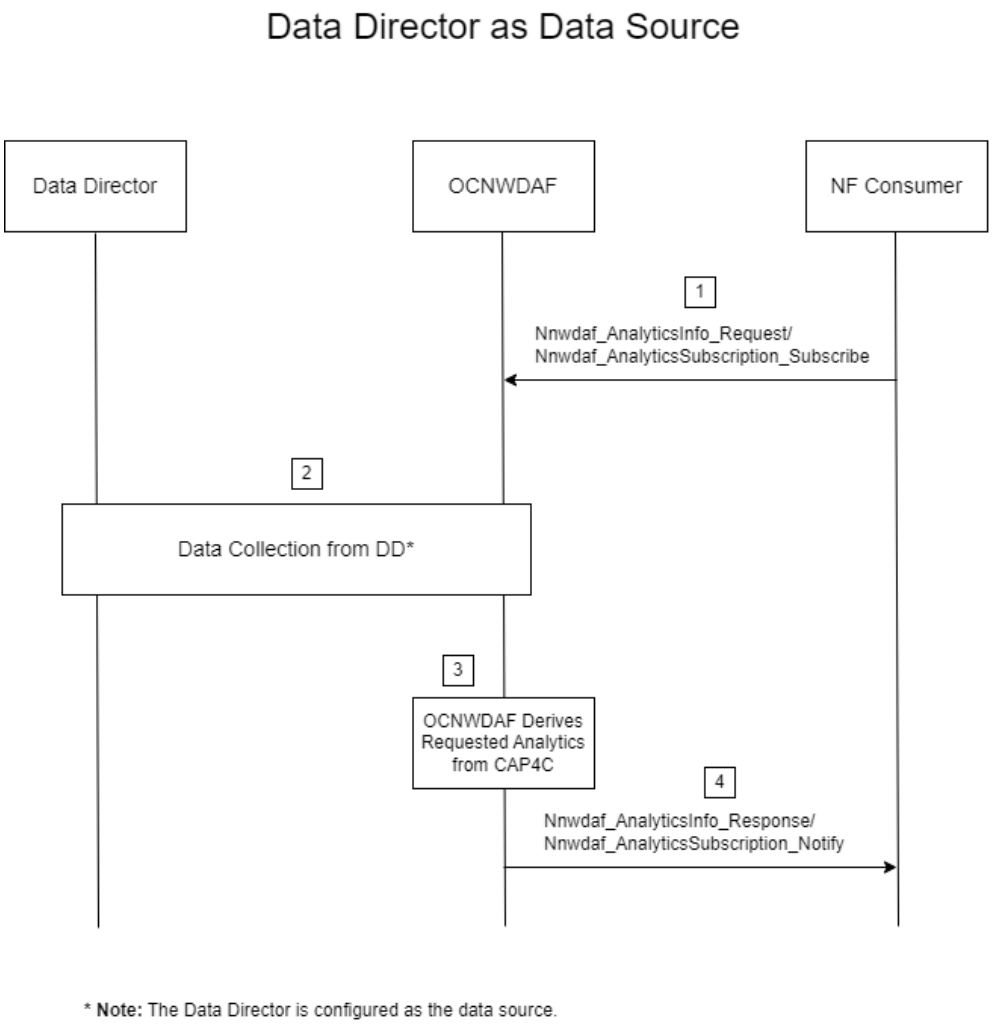


1. The consumer NF sends an analytics request to the OCNWDAF for NF load analytics of a specific NF. The analytics request is either a *Nnwdaf_AnalyticsInfo_Request* or a *Nnwdaf_AnalyticsSubscription_Subscribe* request. The Analytics ID is set to *NF load*, the target for analytics and the analytics filter are also specified in the request. The NF can request statistics or predictions or both and can also provide a time window during which the analytics are generated and shared.
2. The request is authorized and then the OCNWDAF subscribes to the NRF to receive notifications about load and status changes of NF instances identified by the NF ids. The *Nnrf_NFManagement_NFStatusSubscribe* service is used to subscribe for each NF instance.
3. The NRF notifies the OCNWDAF of any changes in the load and status NF instances by using *Nnrf_NFManagement_NFStatusNotify* service.
4. The OCNWDAF derives the requested analytics from CAP4C.
5. The OCNWDAF provides requested NF load analytics to the consumer NF along with the corresponding Validity Period or Area of Interest, using either the *Nnwdaf_AnalyticsInfo_RequestResponse* response or *Nnwdaf_AnalyticsSubscription_Notify* response, based on the consumer NF request.
6. If the consumer NF request is a subscription request, the OCNWDAF generates new analytics based on the Analytics target period or Reporting Threshold specified in the request. The OCNWDAF receives notifications from the NRF whenever there is a change in the NF load of the target NF, accordingly the OCNWDAF generates new analytics information for the consumer NF.

Oracle Communications Network Analytics Data Director (OCNADD) as Data Source

The Oracle Communications Network Analytics Data Director (OCNADD) can be configured as a data collection source for the OCNWDAF.

Figure 7-5 NF Load Analytics Workflow OCNADD as Data Source



> **Note**
>
> During OCNADD deployment, configure the parameter **Include Message with xDR** as **HEADERS_DATA**. Select this option to include xDRs with complete messages. For more information, see "*Select xDR Type Related Info*" in the "*Creating Correlation Configurations procedure*" in the "*Correlation Configurations*" section of the *Oracle Communications Network Analytics Data Director User Guide*.

Below is the workflow description when OCNADD is configured as the data source:

1. The analytics consumer sends an analytics request to the OCNWDAF for NF Load analytics. The analytics request is either an analytics subscription request

(*Nnwdaf_AnalyticsSubscription_Subscribe*) or an analytics information request (*Nnwdaf_AnalyticsInfo_Request*).

2. The OCNWDAF collects the required data such as cell location or session information from the Data Director.
3. The OCNWDAF derives the required analytics from the CAP4C.
4. The OCNWDAF sends the analytics information to the analytics consumer through a *Nnwdaf_AnalyticsSubscription_Notify* or *Nnwdaf_AnalyticsInfo_Request* message.

Configure OCNADD as a Data Source

A specific data set is required from the OCNADD for NF Load analytics, follow the procedure below to configure OCNADD as a data source for NF Load Analytics:

OCNADD Filter Configuration

Configure the OCNADD filter as below to isolate messages sent by the UDM to the NRF by adding the `user-agent` filter condition:

```
#Filter Request
curl -k --location --request POST 'https://ocnaddconfiguration:12590/ocnadd-
configuration/v2/filter' \
 --header 'Content-Type: application/json' \
 --data-raw '{
     "filterConfigurationDtos": [{
             "userName": "Admin",
             "filterInfoDto": {
                 "filterName": "NRFHeartbeat_UDM",
                 "filterConditionDto": [
                    {
                         "conditionName": "service-name",
                         "conditionValue": [
                             "nnrf-nfm/v1/nf-instances"
                         ]
                    }
                    {
                        "user-agent": "udm"
                    }
                    {
                        "methodType":["PATCH"]
                    }
                 ],
                 "filterRule": ["service-name" AND "user-agent" AND
"methodType"],
                 "action": "ALLOW",
                 "status": "ACTIVATE"
             },
             "associationDto": {
                 "associationType": "EGRESS_FILTER",
                 "associationName": [
                     "CAP4C1-FILTERED"
                 ]
             }
         }
     ]
 }'
```

OCNADD Correlation Configuration

Set the following parameters for the correlation service configuration:

- xDR type = SUDR (Single Unit Detailed Record), as transaction correlation is not required.
- includeMessageWithxDR = HEADERS_DATA

OCNADD Correlation Filter for NRF Load

Configure the OCNADD Correlation Filter for NRF Load as below:

```
#Correlation Request
curl -k --location --request POST 'https://ocnaddconfiguration:12590/ocnadd-
configuration/v1/correlation' \
--header 'Content-Type: application/json' \
--data '{
    "correlationConfigDto": {
        "configurationName":"NRFHeartBeatPatch",
        "userName":"Admin",
        "dataStreamStartPoint": "LATEST",
        "inboundDataStreamName":"CAP4C1-FILTERED",
        "outboundDataStreamName":"CAP4C2-CORRELATED",
        "includeMessageWithxDR": "HEADERS_DATA",
        "supportedXdrContents": [
                    "path",
                    "methodType"
                ],
        "xdrType": "SUDR"
    }
}
```

Configure Filters for LCI-OCI Headers

OCNADD filter configuration for capturing the UDM-AMF response messages:

> **Note**
>
> You can use a default correlation configuration for this filter.

```
#Filter Request
curl -k --location --request POST 'https://ocnaddconfiguration:12590/ocnadd-
configuration/v2/filter' \
 --header 'Content-Type: application/json' \
 --data-raw '{
     "filterConfigurationDtos": [{
             "userName": "Admin",
             "filterInfoDto": {
                 "filterName": "UDM_AMF_Response",
                 "filterConditionDto": [
                    {
                        "user-agent": "amf"
                    }
                    {
                        "message-direction": "RxResponse"
                    }
```

```
                ],
                "filterRule": ["user-agent" AND "RxResponse"],
                "action": "ALLOW",
                "status": "ACTIVATE"
            },
            "associationDto": {
                "associationType": "EGRESS_FILTER",
                "associationName": [
                    "CAP4C1-FILTERED"
                ]
            }
        }
    ]
}'
```

N8 Filter Configuration

Configure the N8 filter for NUDM-UECM API calls as below:

```
#Filter Request
curl -k --location --request POST 'https://ocnaddconfiguration:12590/ocnadd-
configuration/v2/filter' \
 --header 'Content-Type: application/json' \
 --data-raw '{
    "filterConfigurationDtos": [{
            "userName": "Admin",
            "filterInfoDto": {
                "filterName": "N8_AMF2UDM",
                "filterConditionDto": [
                   {
                        "path": "registrations/amf-3gpp-access"
                   }
                   {
                       "user-agent": "amf"
                   }
                   {
                       "methodType": [
                           "PUT"
                       ]
                   }
                ],
                "filterRule": ["path" AND "user-agent" AND "methodType"],
                "action": "ALLOW",
                "status": "ACTIVATE"
            },
            "associationDto": {
                "associationType": "EGRESS_FILTER",
                "associationName": [
                    "CAP4C1-FILTERED"
                ]
            }
        }
    ]
}'
```

Correlation Configuration for N8 Filter

Below is the correlation configuration for N8 filter:

```
#Correlation Request
curl -k --location --request POST 'https://ocnaddconfiguration:12590/ocnadd-
configuration/v1/correlation' \
--header 'Content-Type: application/json' \
--data '{
    "correlationConfigDto": {
        "configurationName":"N8AMF2UDMUECMCorrelation",
        "userName":"Admin",
        "dataStreamStartPoint": "LATEST",
        "inboundDataStreamName":"CAP4C1-FILTERED",
        "outboundDataStreamName":"CAP4C2-CORRELATED",
        "correlationMode":"CORRELATION_ID",
        "includeMessageWithxDR": "HEADERS",
        "supportedXdrContents": [
                    "path",
                    "supi",
                    "gpsi",
                    "pei",
                    "methodType",
                    "statusCode",
                    "producerNfType",
                    "consumerId",
                    "consumerFqdn",
                    "producerFqdn",
                    "contentType",
                    "ueId",
                    "snssai",
                    "dnn",
                ],
        "xdrType": "TDR"
    }
}'
```

Enhanced NF Load Analytics with OCNADD as Data Source

The Oracle Communications Network Analytics Data Director (OCNADD) can be configured as a data source for NF load analytics. When OCNADD is configured as a data source, the NF Load Analytics information in the OCNWDAF GUI is enhanced to include information such as Round Trip Time (RTT), Observed Transactions Per Second (OTPS), NF Load information, and Error Rates (only for UDM). A graphical representation of all these NF Load analytics parameters is displayed on the screen. For more information, see NF Load Dashboard.

The NF Load Dashboard is enhanced to display NF Load predictive analytics. You can provide a **Start Time** and **Forecasting Period**, and click **Start Prediction**. The OCNWDAF performs predictive analysis and displays the information on the OCNWDAF GUI. For more information, see NF Load Dashboard.

The OCNWDAF provides a GUI dashboard for selecting, training, and optimizing one or more ML Models for every analytics category. A new ML model, **SARIMAX**, is introduced for NF Load analytics. When this model is selected, configure the following **Model Tuning Parameters**:

- **Enter Moving Average Value - MA(q)**

- **Enter Auto Regressive Value - AR(p)**

For more information, see Machine Learning (ML) Model Selector.

Consumer request to OCNWDAF

A typical consumer request for NF load analytics consists of the following:

- The analytics ID is set to *NF_Load*.
- The Target of Analytics Reporting : Only "any UE" is currently supported.
- Analytics filter information, consisting of the following:
  - S-NSSAI (optional)
  - Either NF Instance IDs or NF Set IDs or NF types are required. The order of precedence is NF Type, NF Instance ID , and then NF Set ID. If all or any two of them exist in the same request, one with the highest precedence is used.
  - List of analytics subsets (optional)
- Preferred level of accuracy (optional)
- Accuracy level per analytics subset (optional)
- Preferred order of results (ascending or descending) (optional)
- Reporting Threshold (optional)
- Analytics target time
- If the consumer has opted for a subscription, the Notification Correlation Id and the Notification Target Address are included.

NF Load Data Collection

The OCNWDAF collects the following NF data to generate NF load analytics:

Table 7-15 Data Collection

Information Collected	Source	Description
NF Load	NRF	The load of specific NF instances in their NF profile.
NF Status	NRF	The status of specific NF instances. The status can be registered, suspended or not discoverable.

> **Note**
>
> - OCNWDAF can request NRF for data related to NF instances.
> - OCNWDAF can correlate the NF resources configuration with NF resource usage for generating the analytics output.

For more information see Data Collection from NRF.

Output NF Load Analytics

The following analytics information is obtained:

- NF load statistics information
- NF load prediction information

The NF load statistics include the following information:

Table 7-16 NF Load Statistics

Parameter	Data Type	P	Cardinality	Description
List of resource status	Integer	M	1 up to the maximum value	List of observed load information for each NF instance along with the corresponding NF id or NF Set ID (as applicable).
NF Type	NFType	M	1	Type of the NF instance.
NF Instance ID	NfInstanceId	M	1	Identification of the NF instance.
NF Set ID	NfSetId	O	0 to 1	Identification of the NF instance set
NF Status	NfStatus	O	0 to 1	The availability status of the NF in the Analytics target period. It is expressed as a percentage of time per status value. The possible values are registered, unregistered, or undiscoverable.
NF resource usage	Integer	C	0 to 1	The average usage of assigned resources (CPU, memory, and disk).
NF load	Integer	C	0 to 1	The average load on the NF instance during the analytics target period.
NF peak load	Integer	O	0 to 1	The maximum load on the NF instance during the analytics target period.
NF load (per area of interest)	Integer	C	0 to 1	The average load of the NF instances over the area of interest.
S-NSSAI	Snssai	C	0 to 1	Identifies the S-NSSAI.

The NF load prediction include the following information:

Table 7-17 NF Load Statistics

Parameter	Data Type	P	Cardinality	Description
List of resource status	Integer	M	1 up to the maximum value	List of observed load information for each NF instance along with the corresponding NF id or NF Set ID (as applicable).
NF Type	NFType	M	1	Type of the NF instance.
NF Instance ID	NfInstanceId	M	1	Identification of the NF instance.
NF Set ID	NfSetId	O	0 to 1	Identification of the NF instance set
NF Status	NfStatus	O	0 to 1	The availability status of the NF in the Analytics target period. It is expressed as a percentage of time per status value. The possible values are registered, unregistered, or undiscoverable.
NF resource usage	Integer	C	0 to 1	The average usage of assigned resources (CPU, memory, and disk).
NF load	Integer	C	0 to 1	The average load on the NF instance during the analytics target period.
NF peak load	Integer	O	0 to 1	The maximum load on the NF instance during the analytics target period.
Confidence	Uinteger	C	0 to 1	Indicates the confidence of this prediction.
NF load (per area of interest)	Integer	C	0 to 1	The average load of the NF instances over the area of interest.
S-NSSAI	Snssai	C	0 to 1	Identifies the S-NSSAI.

Enumeration NFType

Table 7-18 NFType

Enumeration Value	Description
"NRF"	Network Function: NRF
"UDM"	Network Function: UDM
"AMF"	Network Function: AMF
"SMF"	Network Function: SMF
"AUSF"	Network Function: AUSF
"NEF"	Network Function: NEF
"PCF"	Network Function: PCF
"SMSF"	Network Function: SMSF
"NSSF"	Network Function: NSSF
"UDR"	Network Function: UDR
"LMF"	Network Function: LMF
"GMLC"	Network Function: GMLC
"5G_EIR"	Network Function: 5G-EIR
"SEPP"	Network Entity: SEPP
"UPF"	Network Function: UPF
"N3IWF"	Network Function and Entity: N3IWF
"AF"	Network Function: AF
"UDSF"	Network Function: UDSF
"BSF"	Network Function: BSF
"CHF"	Network Function: CHF
"NWDAF"	Network Function: NWDAF
"PCSCF"	Network Function: P-CSCF
"CBCF"	Network Function: CBCF
"UCMF"	Network Function: UCMF
"HSS"	Network Function: HSS
"SOR_AF"	Network Function: SOR-AF
"SPAF"	Network Function: SP-AF
"MME"	Network Function: MME
"SCSAS"	Network Function: SCS/AS
"SCEF"	Network Function: SCEF
"SCP"	Network Entity: SCP
"NSSAAF"	Network Function: NSSAAF
"ICSCF"	Network Function: I-CSCF
"SCSCF"	Network Function: S-CSCF
"DRA"	Network Function: DRA
"IMS_AS"	Network Function: IMS-AS
"AANF"	Network Function: AAnF
"5G_DDNMF"	Network Function: 5G DDNMF
"NSACF"	Network Function: NSACF
"MFAF"	Network Function: MFAF
"EASDF"	Network Function: EASDF
"DCCF"	Network Function: DCCF
"MB_SMF"	Network Function: MB-SMF

Table 7-18 (Cont.) NFType

Enumeration Value	Description
"TSCTSF"	Network Function: TSCTSF
"ADRF"	Network Function: ADRF
"GBA_BSF"	Network Function: GBA BSF
"CEF"	Network Function: CEF
"MB_UPF"	Network Function: MB-UPF
"NSWOF"	Network Function: NSWOF
"PKMF"	Network Function: PKMF
"MNPF"	Network Function: MNPF
"SMS_GMSC"	Network Function: SMS-GMSC
"SMS_IWMSC"	Network Function: SMS-IWMSC
"MBSF"	Network Function: MBSF
"MBSTF"	Network Function: MBSTF
"PANF"	Network Function: PANF

Type NfInstanceId

Table 7-19 NfInstanceId

Type Name	Type Definition	Description
NfInstanceId	String	String uniquely identifying a NF instance. The format of the NF Instance ID shall be a Universally Unique Identifier (UUID) version 4, as described in IETF RFC 4122 [15].

Type NfSetId

Table 7-20 NfSetId

Type Name	Type Definition	Description

NfSetId	String	NF Set Identifier. Formatted as below:
		`set<SetID>.<nftype>set.5gc.mnc<MNC>.mcc<MCC>`
		or
		`set<SetID>.<NFType>set.5gc.nid<NID>.mnc<MNC>.mcc<MCC>`
		Example:
		`setxyz.smfset.5gc.mnc012.mcc345`

Type NfStatus

Table 7-21 NfStatus

Attribute name	Data type	P	Cardinality	Description
statusRegistered	SamplingRatio	C	0 to 1	Percentage of time with status “registered”
statusUnregistered	SamplingRatio	C	0 to 1	Percentage of time with status “unregistered”
statusUndiscoverable	SamplingRatio	C	0 to 1	Percentage of time with status “undiscoverable”

> **Note**
>
> The total of status values should be equal or lower than 100%. At least one value is provided.

Type Snssai

Table 7-22 Snssai

Attribute name	Data type	P	Cardinality	Description
sst	Uinteger	M	1	Represents the Slice or Service Type. It indicates the expected Network Slice behavior in terms of features and services. The allowed range is 0 to 255.
sd	String	O	0 to 1	Represents the Slice Differentiator in the 3-octet string format.

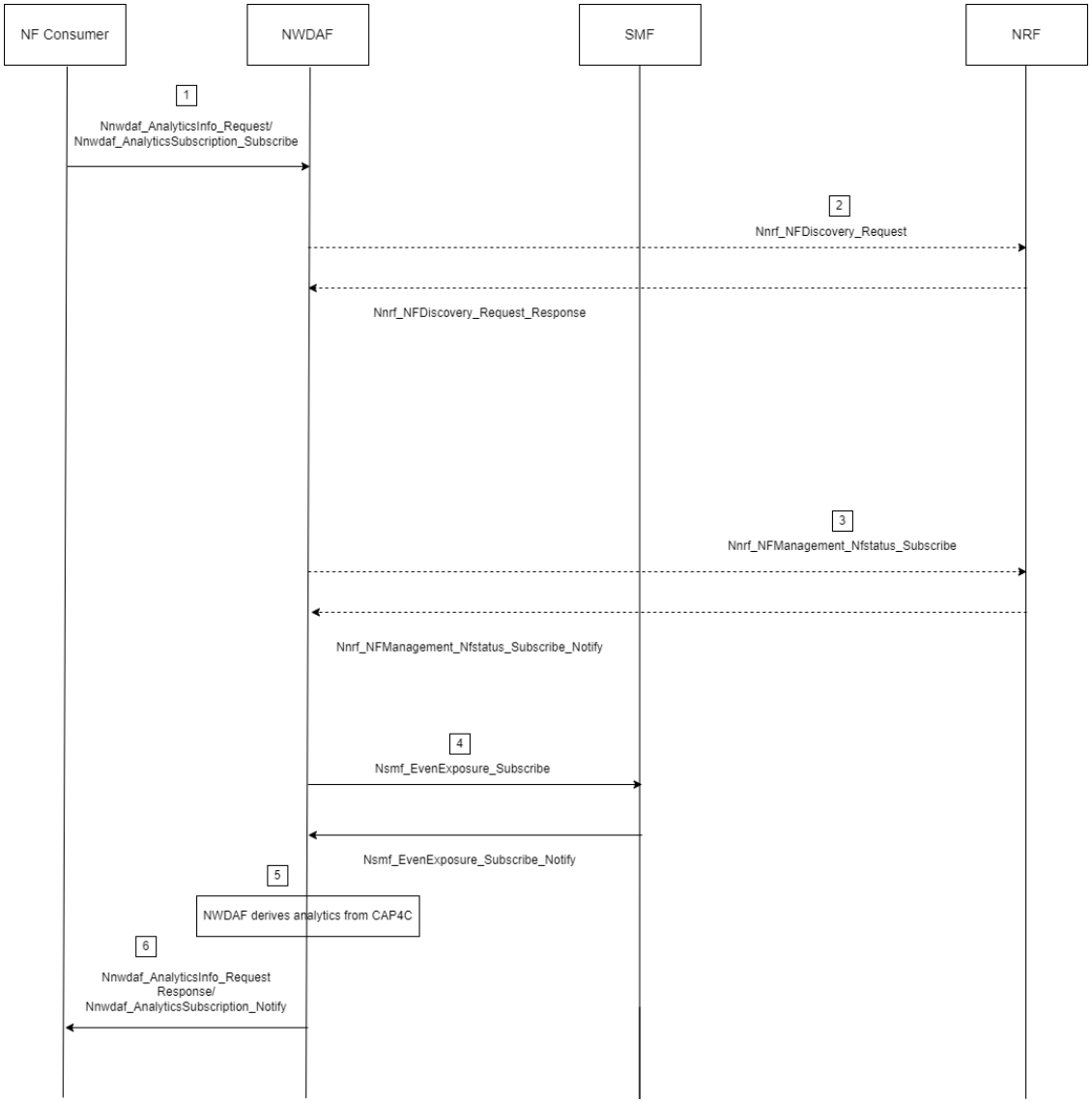
7.5 Slice Load Level Analytics

The OCNWDAF provides Slice Load Level analytics to the consumers at the Network Slice level. To generate this analytics report, the OCNWDAF need not have information about the subscribers in the slice, the slice load level analytics information is not subscriber specific. The OCNWDAF notifies slice specific network status analytics information to the subscribed consumers. The Analytics Subscription service and Analytics Information service expose the slice load level analytics to the consumers.

The Analytics ID used for the slice load level information is “SLICE_LOAD_LEVEL”(for Analytics Subscription Service) or "LOAD_LEVEL_INFORMATION” (for Analytics Information Service).

> **Note**
>
> In the current release, only one network instance per slice is supported.

Figure 7-6 Slice Load Level Workflow



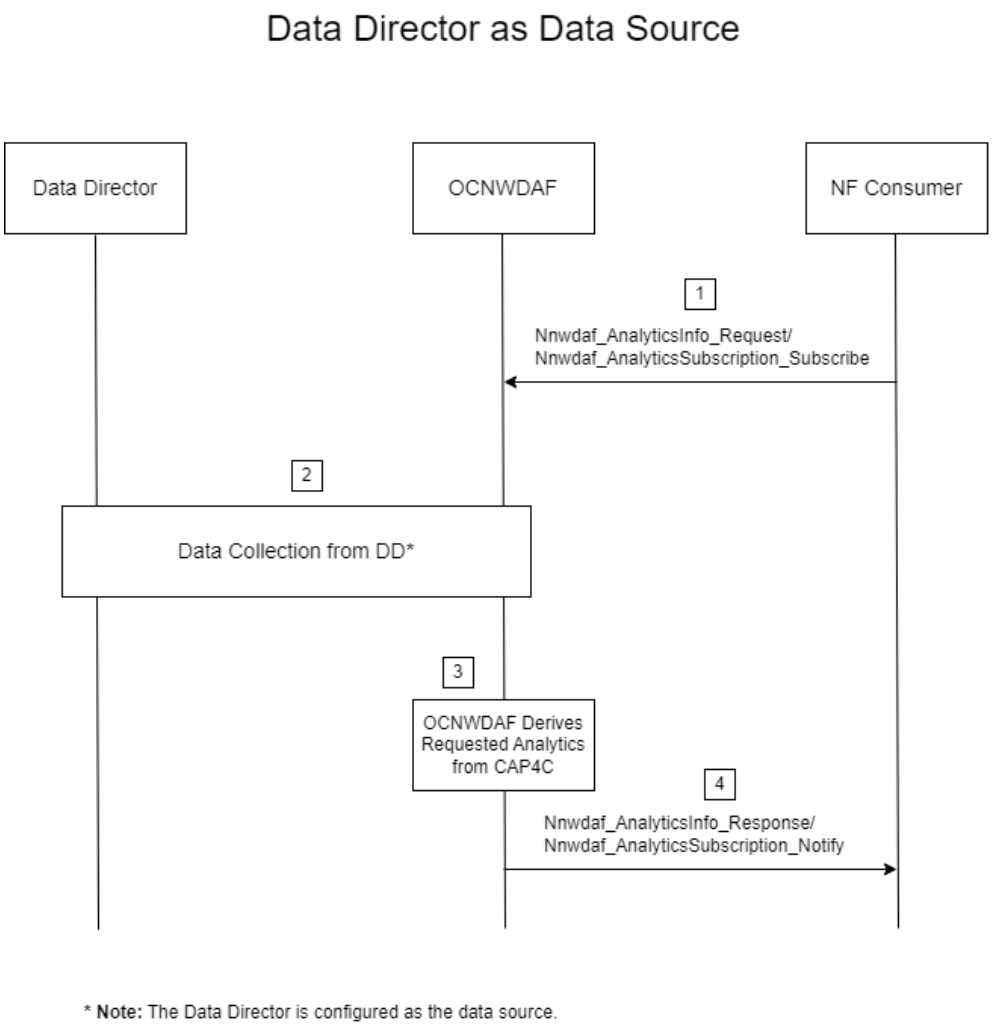
1. A consumer subscribes to an OCNWDAF (*Nnwdaf_AnalyticsSubscription_Subscribe*) or sends a request to an OCNWDAF (*Nnwdaf__AnalyticsInfo_Request*) with the Analytics ID and optional filters such as S-NSSAI, Area of Interest and Load level threshold value.
2. The OCNWDAF collects input data from the NRF to derive resource usage statistics and predictions for a Network Slice instance. It sends a *Nnrf_NFDiscovery_Request* to the NRF and receives a *Nnrf_NFDiscovery_Response* from the NRF.
3. The OCNWDAF invokes a *Nnrf_NFManagement_NFstatus_Subscribe* request to get the NFs status information, the NRF responds with a *Nnrf_NFManagement_NFstatus_Subscribe_Notify* with requested information.

4. The OCNWDAF subscribes to the SMF's event exposure service to collect data on the number of PDU sessions currently registered on a specific Network Slice (if the slice is available). The PDU session establishment or release event information is collected.
5. The OCNWDAF derives the slice load analytics from the CAP4C.
6. The OCNWDAF delivers the analytics information to the consumers by invoking *OCNWDAF_AnalyticsSubscription_Notify* or *OCNWDAF_AnalyticsInfo_Request* response.

Oracle Communications Network Analytics Data Director (OCNADD) as Data Source

The Oracle Communications Network Analytics Data Director (OCNADD) can be configured as a data collection source for the OCNWDAF.

Figure 7-7 Slice Load Level Workflow OCNADD as Data Source



* **Note:** The Data Director is configured as the data source.

> **Note**
>
> During OCNADD deployment, configure the parameter **Include Message with xDR** as **HEADERS_DATA**. Select this option to include xDRs with complete messages. For more information, see "*Select xDR Type Related Info*" in the "*Creating Correlation Configurations procedure*" in the "*Correlation Configurations*" section of the *Oracle Communications Network Analytics Data Director User Guide*.

Below is the workflow description when OCNADD is configured as the data source:

1. The analytics consumer sends an analytics request to the OCNWDAF for Slice Load Level analytics. The analytics request is either an analytics subscription request (*Nnwdaf_AnalyticsSubscription_Subscribe*) or an analytics information request (*Nnwdaf_AnalyticsInfo_Request*).
2. The OCNWDAF collects the required data such as cell location or session information from the Data Director.
3. The OCNWDAF derives the required analytics from the CAP4C.
4. The OCNWDAF sends the analytics information to the analytics consumer through a *Nnwdaf_AnalyticsSubscription_Notify* or *Nnwdaf_AnalyticsInfo_Request* message.

Consumer request to OCNWDAF

A consumer request for Slice Load Level analytics contains:

- Analytics ID: “SLICE_LOAD_LEVEL” (for Analytics Subscription Service) or LOAD_LEVEL_INFORMATION” (for Analytics Information Service).
- Analytics filter information:
  - S-NSSAI: The S-NSSAI is the network slice identifier.
  - Area of Interest (AoI) (Optional)
  - Load level threshold value
  - List of NF types (Optional)
  - List of analytics subsets (Optional)
  - Maximum number of objects (Optional)

The OCNWDAF reports when the load level of the network slice crosses the threshold value specified in the network analytics subscription service.

The analytics is generated on specified event detection (Network Analytics Information Service) or if the defined threshold is reached (Network Analysis Subscription Service). In this case, the event and threshold are related to the load level in the slice.

Slice Load Level Analytics Report

The following analytics information is obtained:

- Network Slice load statistics
- Network Slice load predictions

The Network Slice load statistics include the following information:

Table 7-23 Network Slice Instance Load Statistics

Parameter	Data type	P	Cardinality	Description
Load Level Information	loadLevelInformation	M	1 up to the maximum value	Load level information of the network slice calculated per time period. Load level is based on the maximum number of UEs or sessions that the slice can support and is limited by the maximum configured UEs or sessions. The load level value is the either the value of "Percent UE" or "Percent Session", whichever is the highest.
S-NSSAI	String	M	0 to 1	The S-NSSAI is the network slice identifier. This information is obtained from the analytics request.
Number of UE Registrations	Integer	M	1 up to the maximum value	The number of UE registrations within the Network Slice.
Percent UE	Integer	M	1 up to the maximum value	Is a proprietary value obtained by the percentage of Number of UE registrations in the slice and the configured value of maximum UEs per S-NSSAI.
Number of PDU Sessions	Integer	M	1 up to the maximum value	The number of PDU Sessions established within the Network Slice.
Percent Sessions	Integer	M	1 up to the maximum value	Is a proprietary value obtained by the percentage of Number of PDU Sessions in the slice and the configured value of maximum sessions per S-NSSAI.

Table 7-23 (Cont.) Network Slice Instance Load Statistics

Parameter	Data type	P	Cardinality	Description
Exceed Load Level Threshold	Boolean	M	True or False	Is true when the load level threshold is crossed within the time period of the analytics report.

Table 7-24 Type LoadLevelInformation

Type Name	Type Definition	Description
LoadLevelInformation	Integer	Load level information of the network slice

The Network Slice load predictions include the following information:

Table 7-25 Network Slice Instance Load Predictions

Parameter	Data type	P	Cardinality	Description
Load Level Information	loadLevelInformation	M	1 up to the maximum value	Load level information of the network slice calculated per time period. Load level is based on the maximum number of UEs or sessions that the slice can support and is limited by the maximum configured UEs or sessions. The load level value is the either the value of "Percent UE" or "Percent Session", whichever is the highest.
S-NSSAI	String	M	0 to 1	The S-NSSAI is a network slice identifier.
Number of UE Registrations	Integer	M	1 up to the maximum value	The number of UE registrations in the Network Slice.

Table 7-25 (Cont.) Network Slice Instance Load Predictions

Parameter	Data type	P	Cardinality	Description
Percent UE	Integer	M	1 up to the maximum value	Is a proprietary value obtained by the percentage of Number of UE registrations in the slice and the configured value of maximum UEs per S-NSSAI.
Number of PDU Sessions	Integer	M	1 up to the maximum value	The number of PDU Session established in the Network Slice.
Percent Sessions	Integer	M	1 up to the maximum value	Is a proprietary value obtained by the percentage of Number of PDU Sessions in the slice and the configured value of maximum sessions per S-NSSAI.
Exceed Load Level Threshold	Boolean	M	True or False	Is true when the load level threshold is crossed within the time period of the analytics report.
Confidence	Uinteger	C	0 to 1	Indicates the confidence of this prediction. It has a value range from Minimum "0" up to Maximum "100".

7.6 UE Related Analytics

OCNWDAF provides the following UE related analytics:

- UE mobility analytics. For more information, see UE Mobility Analytics.
- UE abnormal behavior analytics (unexpected UE location and proprietary geofencing feature). For more information, see User Equipment (UE) Abnormal Behavior Analytics.

7.6.1 UE Mobility Analytics

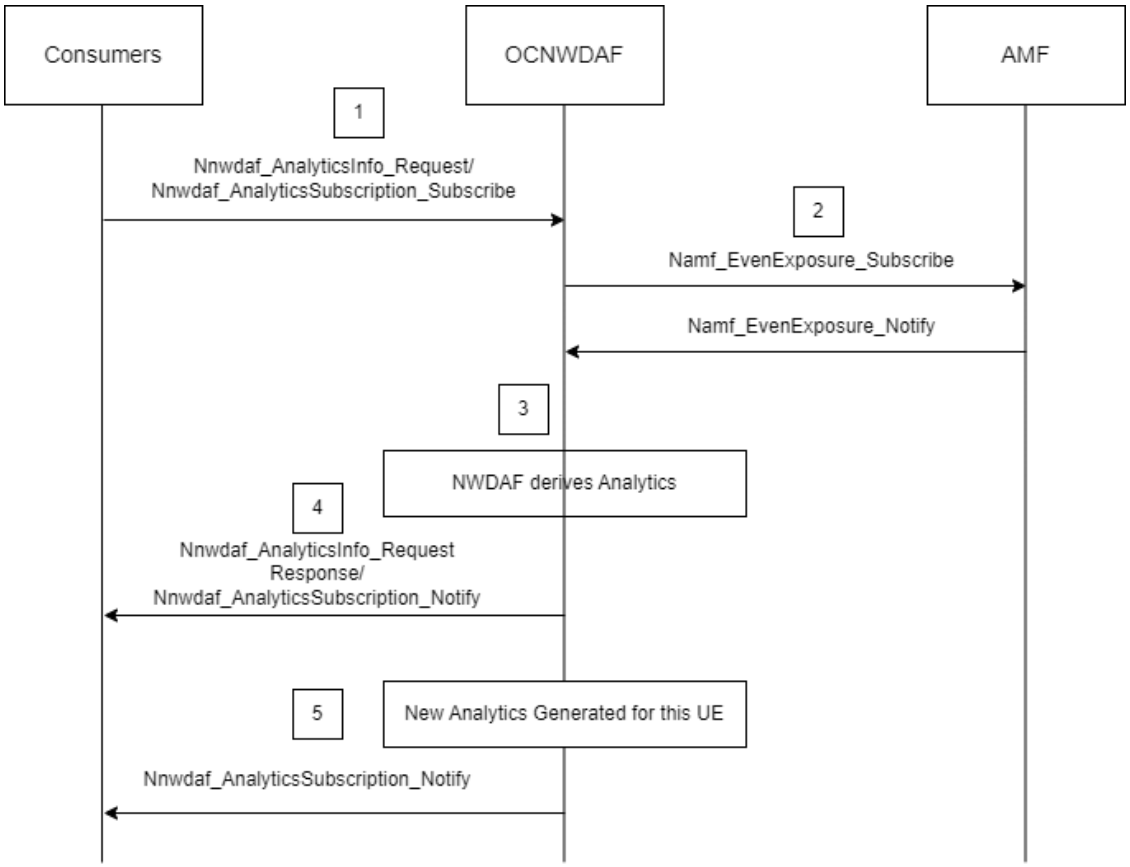
OCNWDAF provides UE mobility statistical or predictive analytics to allow consumers to do the following:

- Collect UE mobility related information from 5G NFs (such as AMF).
- Perform data analytics on the collected information to obtain UE mobility descriptive or predictive analytics.

> **Note**
>
> The detailed information collected by the OCNWDAF can be network data from 5GCs.
>
> - UE mobility related network data collected from 5GC is UE location information.

UE Mobility Workflow

Figure 7-8 UE Mobility Workflow



1. The consumer sends a request to OCNWDAF for analytics on a specific UE or a group of UEs, using either the *Nnwdaf_AnalyticsInfo* or the *Nnwdaf_AnalyticsSubscription* service. The consumer can request statistics or predictions or both. The type of analytics is set to UE mobility information. The NF provides the UE ID or Internal Group ID in the Target of Analytics Reporting.
2. If the request is authorized, and in order to provide the requested analytics, OCNWDAF may subscribe to events with all the serving AMFs for notification of location changes.

> **Note**
>
> This step may get skipped when OCNWDAF has the requested analytics available already.

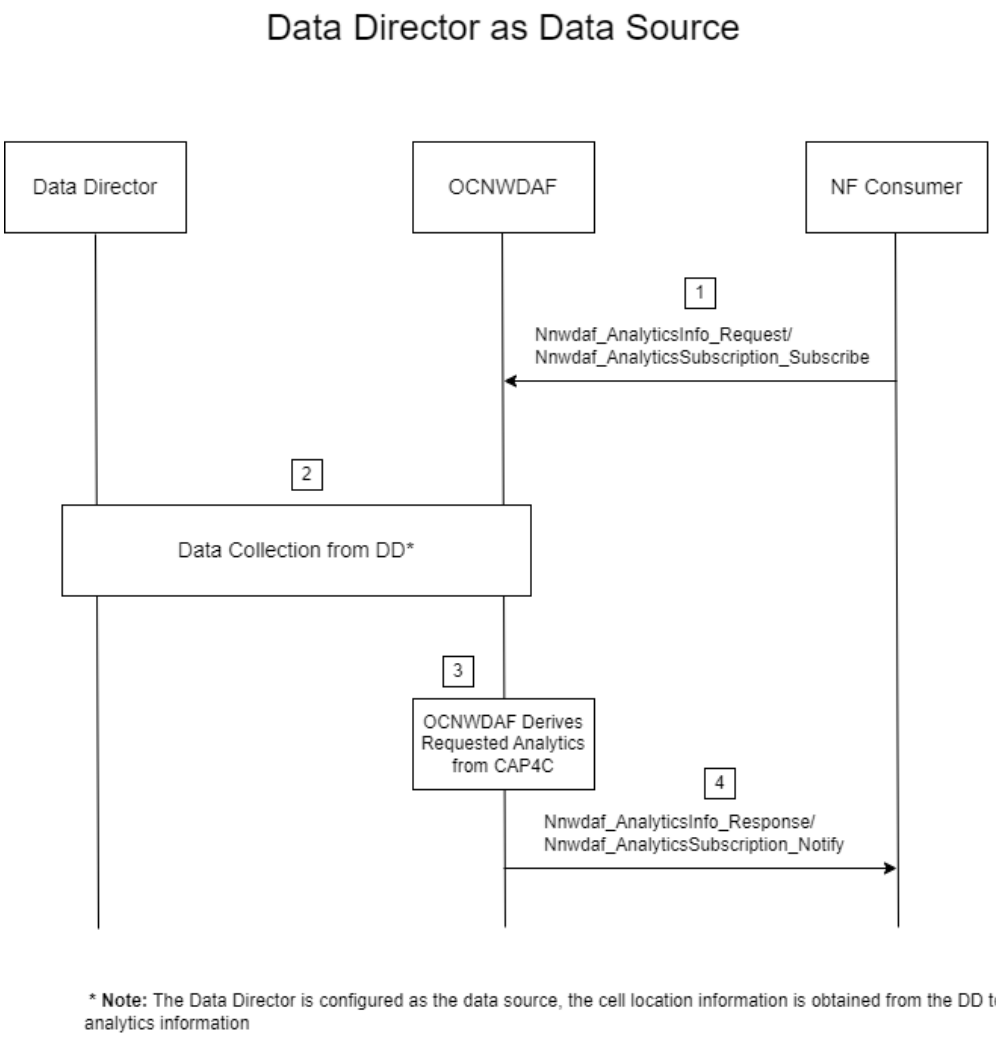
> **Note**
>
> OCNWDAF determines the AMF serving the UE or the group of UEs as described in *3GPP 23.288 6.2.2.1*.

3. OCNWDAF derives the requested analytics from CAP4C.
4. OCNWDAF provides the requested UE mobility analytics to the consumer, using either *Nnwdaf_AnalyticsInfo_Request* response or *Nnwdaf_AnalyticsSubscription_Notify*.
5. If the consumer has subscribed to receive notifications for UE mobility analytics, after receiving event notification from the AMFs subscribed by OCNWDAF , OCNWDAF generates new analytics and provides them to the NF through a *Nnwdaf_AnalyticsSubscription_Notify* response.

Oracle Communications Network Analytics Data Director (OCNADD) as Data Source

The Oracle Communications Network Analytics Data Director (OCNADD) can be configured as a data collection source for the OCNWDAF.

Figure 7-9 UE Mobility Workflow with OCNADD as Data Source



Below is the workflow description when OCNADD is configured as the data source:

1. The analytics consumer sends an analytics request to the OCNWDAF for UE Mobility analytics. The analytics request is either an analytics subscription request (*Nnwdaf_AnalyticsSubscription_Subscribe*) or an analytics information request (*Nnwdaf_AnalyticsInfo_Request*).
2. The OCNWDAF collects the required data such as cell location or session information from the Data Director.
3. The OCNWDAF derives the required analytics from the CAP4C.
4. The OCNWDAF sends the analytics information to the analytics consumer through a *Nnwdaf_AnalyticsSubscription_Notify* or *Nnwdaf_AnalyticsInfo_Request* message.

Consumer Request to OCNWDAF

A consumer request for this analytics information contains:

- Analytics ID: “UE Mobility”
- The following filters can be specified in the subscription request:
  - A single UE or a group of UEs (the Target of analytics reporting)
  - Analytics target period indicating the time period over which the statistics or predictions are requested
  - Preferred level of accuracy of the analytics (low or high)
  - A Notification Correlation ID and Notification Target Address in a subscription

Output UE Mobility Analytics

The following UE mobility analytics information is obtained by OCNWDAF:

- UE mobility descriptive analytics
- UE mobility predictive analytics

The following table lists the UE mobility descriptive analytics:

Table 7-26 UE mobility descriptive analytics

Parameter	Data type	P	Cardinality	Description
Time slot entry	DateTime	O	0 to 1	This attribute identifies the timestamp when the UE arrives at the location.
Time slot start	ScheduledCommunicationTime	O	0 to 1	Identifies time of the day and day of the week which are valid within the observation period when the UE moves.

Table 7-26 (Cont.) UE mobility descriptive analytics

Parameter	Data type	P	Cardinality	Description
Duration	DurationSec	M	1	This attribute identifies the time duration the UE stays in the location. If the analytics result applies for a group of UEs, it indicates the average duration for the group of UEs.
UE location	UserLocation	M	1	This attribute contains the detailed location, the ueLocationTimestamp attribute in the 3GPP access type of UserLocation data type shall not be provided.
UE location Ratio	SamplingRatio	C	0 to 1	Indicates the percentage of UEs in the group (in case of a UE group)

The following table lists the UE mobility predictive analytics:

Table 7-27 UE mobility predictive analytics

Parameter	Data type	P	Cardinality	Description
Time slot entry	DateTime	O	0 to 1	This attribute identifies the timestamp when the UE arrives at the location.
Time slot start	ScheduledCommunicationTime	O	0 to 1	Identifies time of the day and day of the week which are valid within the observation period when the UE moves.

Table 7-27 (Cont.) UE mobility predictive analytics

Parameter	Data type	P	Cardinality	Description
Duration	DurationSec	M	1	This attribute identifies the time duration the UE stays in the location. If the analytics result applies for a group of UEs, it indicates the average duration for the group of UEs.
UE location	UserLocation	M	1	Indicates the predicted location during the analytics target period.
Confidence	Uinteger	C	0 to 1	Indicates the confidence of a prediction
Ratio	SamplingRatio	C	0 to 1	Indicates the percentage of UEs in the group (in case of a UE group)

Note

- When the target of analytics reporting is an individual UE, for example, one UE ID (SUPI) is included, OCNWDAF provides the analytics mobility result (list of (predicted) time slots) to the service consumer(s) for the UE.
- The results for UE groups address the group globally. The ratio is the proportion of UEs in the group at a given location at a given time.
- The time slots are provided by order of time, possibly overlapping. The locations are provided by decreasing value of ratio for a given time slot. The sum of all ratios on a given time slot must be equal or less than 100%. Depending on the list size limitation, the least probable locations on a given analytics target period may not be provided.

7.6.2 User Equipment (UE) Abnormal Behavior Analytics

OCNWDAF provides UE abnormal behavior analytics that allow consumers to identify a specific UE or a group of UEs with abnormal behavior.

The UE abnormal behavior analytics consumer subscribes analytics about abnormal behavior from OCNWDAF based on the UE subscription, network configuration, or application layer request.

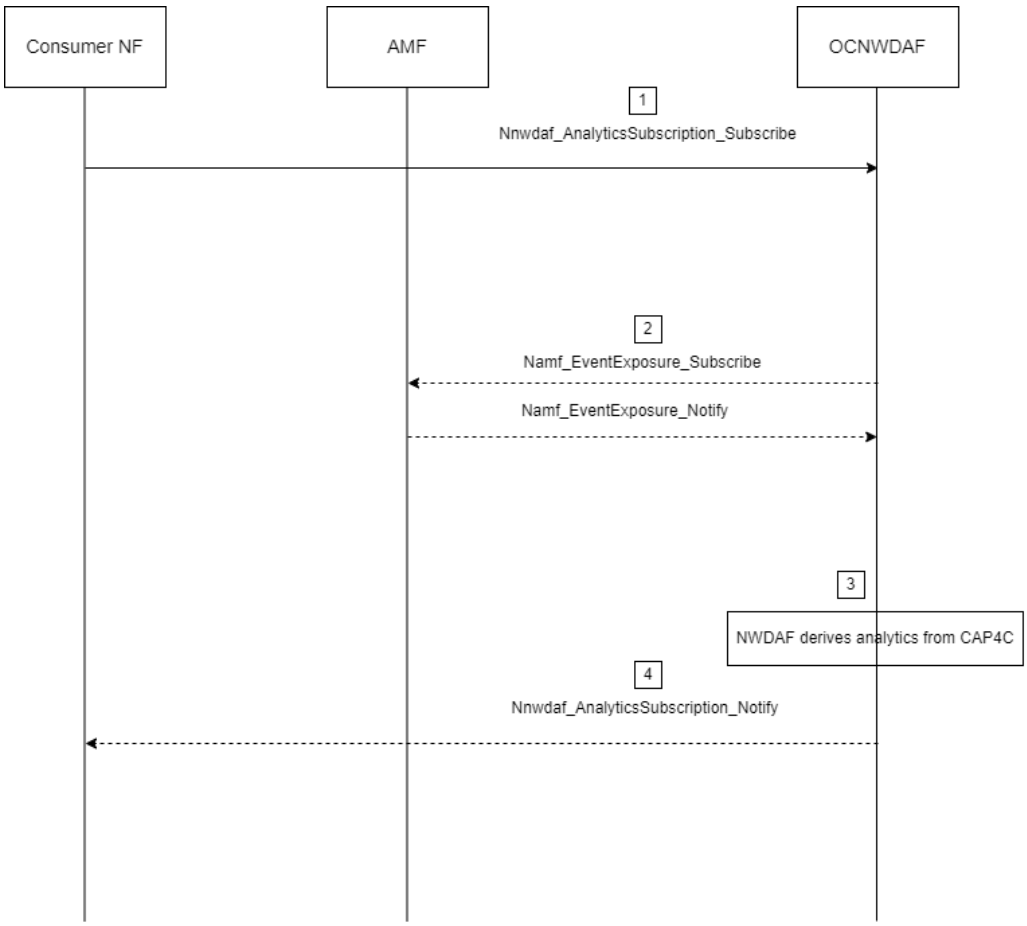
OCNWDAF performs data analytics on abnormal behavior provided there is a related subscription.

OCNWDAF provides the following types of UE abnormal behavior analytics:

- Unexpected UE location: The UE location is monitored to determine if the UE is an unexpected location.
- Geofencing: Geofences are virtual fences or perimeters around physical locations, they can be used to trigger events when a UE enters or exits the region.

UE Abnormal Behavior Workflow

Figure 7-10 UE Abnormal Behavior Workflow



1. A consumer NF subscribes to OCNWDAF using *Nnwdaf_AnalyticsSubscription_Subscribe* (Analytics ID set to "Abnormal behavior", Target of Analytics Reporting set to Internal-Group-Identifier, any UE or SUPI, Analytics Filter Information).

   A consumer NF subscribes to abnormal behavior notification from the OCNWDAF for a group of UEs, any UE, or a specific UE. The Analytics ID indicates OCNWDAF to identify misused or hijacked UEs through abnormal behavior analytics.

2. The OCNWDAF sends a *Namf_EventExposure_Subscribe* message to the AMF. OCNWDAF sends subscription requests to the related AMF to collect UE behavioral information if it has not subscribed such data.

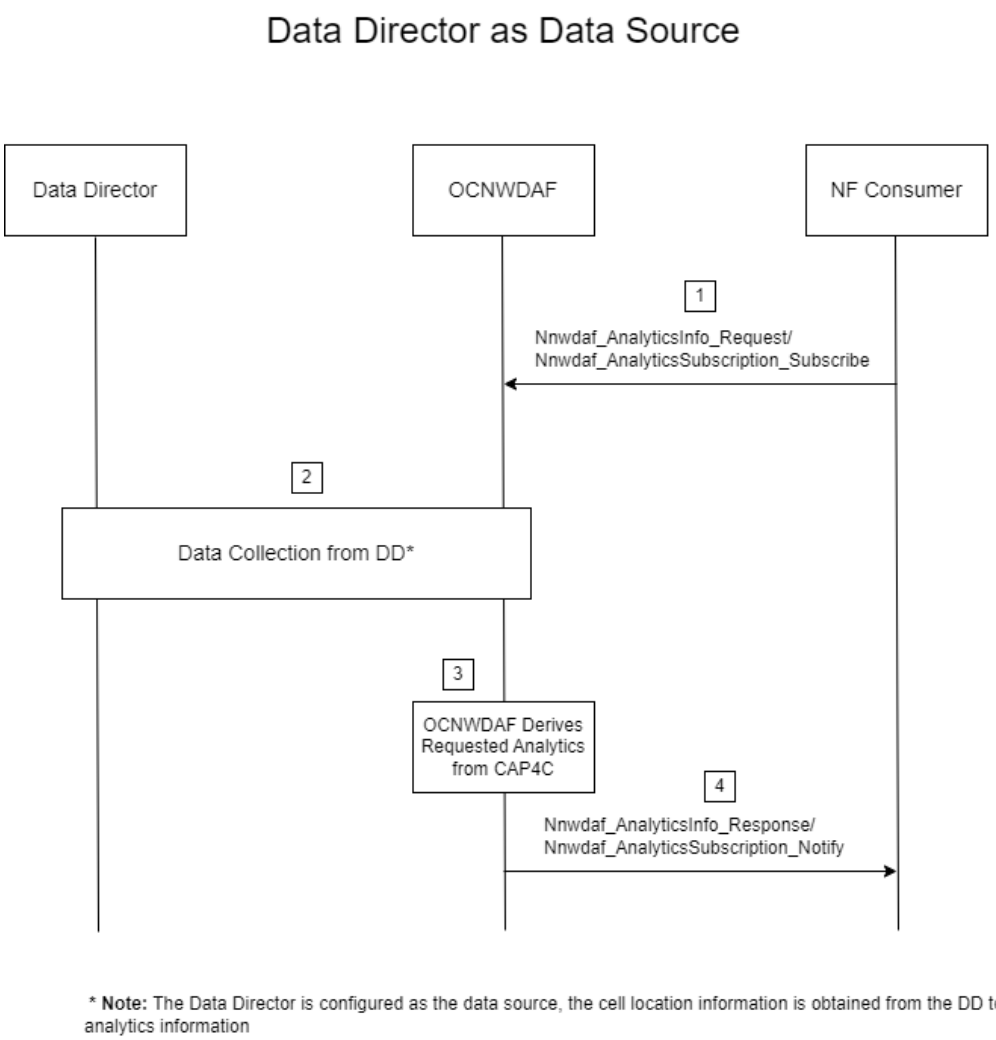
> **Note**
>
> OCNWDAF determines the related AMF(s). The AMF sends event reports to OCNWDAF based on the report requirements contained in the subscription request received from OCNWDAF.
> If requested by OCNWDAF through Event Filter(s), the AMF checks whether the UE's behavior matches its expected UE behavioral information. In this case, the AMF sends event reports to OCNWDAF only when it detects that the UE's behavior deviated from its expected UE behavior.

3. OCNWDAF derives the analytics information from CAP4C.
4. OCNWDAF sends *Nnwdaf_AnalyticsSubscription_Notify* (Analytics ID, Exception ID, Internal-Group-Identifier or SUPI, Exception level) to the consumer NF.

Oracle Communications Network Analytics Data Director (OCNADD) as Data Source

The Oracle Communications Network Analytics Data Director (OCNADD) can be configured as a data collection source for the OCNWDAF.

Figure 7-11 UE Abnormal Behavior Workflow with OCNADD as Data Source



Below is the workflow description when OCNADD is configured as the data source:

1. The analytics consumer sends an analytics request to the OCNWDAF for UE Abnormal Behavior analytics. The analytics request is either an analytics subscription request (*Nnwdaf_AnalyticsSubscription_Subscribe*) or an analytics information request (*Nnwdaf_AnalyticsInfo_Request*).
2. The OCNWDAF collects the required data such as cell location or session information from the Data Director.
3. The OCNWDAF derives the required analytics from the CAP4C.
4. The OCNWDAF sends the analytics information to the analytics consumer through a *Nnwdaf_AnalyticsSubscription_Notify* or *Nnwdaf_AnalyticsInfo_Request* message.

Consumer request to OCNWDAF

A consumer request for this analytics information contains:

- Analytics ID: “Abnormal Behavior”
- The target of analytics reporting which can be a single "UE" or "any UE"
- Target time period of the request
- Expected UE behavior parameters, these parameters are used to define the geofencing area.
- Expected analytics type
- List of exception IDs: List of exception IDs indicates the specific analytics requested by the consumer.

> **Note**
>
> Expected analytics type and list of Exception IDs are mutually exclusive, only one of them are specified in the request. The following table provides information about the correlation between expected analytics type and exception IDs:
>
> **Table 7-28 Expected analytics type and Exception IDs**
>
> | Expected analytics type | Exception IDs |
> |---|---|
> | Mobility | – Unexpected UE location
– Geofencing |

- The analytics filter should at least include S-NSSAI (if the target of analytics reporting is any UE)
- Area of interest
- Application ID
- Optionally, maximum number of objects and maximum number of SUPIs
- Notification Correlation ID and Target Address in the subscription.

UE Geofencing Analytics

Geofences are virtual fences around physical locations. Geofences can be used to trigger events when a UE enters or exits the defined region. Geofences are defined by using the *ExpectedUeBehaviourData* parameter in the analytics request. A proprietary exception ID

"UE_GEOFENCE" is defined to obtain geofencing analytics information. On receiving an analytics request from a consumer, the OCNWDAF detects if the UE location is within the fence or outside the fence or if the UE location is unknown, and accordingly the OCNWDAF provides the analytics report to the consumer.

When OCNWDAF detects UEs that deviate from the expected behavior, for example, in case an unexpected UE location or an abnormal traffic pattern is displayed, the OCNWDAF notifies the consumer with UE Abnormal Behavior Analytics.

UE Abnormal Behavior Analytics

The following UE abnormal behavior analytics information is obtained by OCNWDAF:

Table 7-29 UE abnormal behavior analytics

Parameter	Data type	Mandatory or Optional	Cardinality	Description
excep	Exception	M	1	Contains the exception information.
Exception ID	ExceptionId	M	1	Indicates the Exception ID. For analytics related to geofencing, the exception ID is "UE_GEOFENCE"
Exception Level	Integer	O	0 to 1	Measured level, compared to the threshold
Exception trend	ExceptionTrend	O	0 to 1	The supported values are "IN_FENCE", "OUT_FENCE" or "UNKNOWN", based on the UE location with respect to the geofencing area.
GroupId	Array	O	1 up to the maximum value	Indicates the internal group identifier
SUPI list	Array	C	1 up to the maximum value	Indicates the SUPIs of the UEs affected with Exception
Ratio	SamplingRatio	C	0 to 1	Indicates the estimated percentage of the UEs affected by Exception within the target of analytics reporting

Table 7-29 (Cont.) UE abnormal behavior analytics

Parameter	Data type	Mandatory or Optional	Cardinality	Description
sampRatio	SamplingRatio	O	0 to 1	Indicates the estimated number of UEs affected by Exception (applicable when Target of Analytics Reporting = "any UE")
dnn	Dnn	C	0 to 1	Identifies DNN, a full DNN with both the Network Identifier and Operator Identifier, or a DNN with the Network Identifier only. Shall be present if the "dnns" was provided within EventSubscription during the subscription for event notification procedure.
snssai	Snssai	C	0 to 1	Identifies the network slice information. Shall be present if the "snssais" was provided within EventSubscription during the subscription for event notification procedure.
confidence	Uinteger	C	0 to 1	Indicates the confidence of the prediction.

Enumeration ExceptionId

Table 7-30 ExceptionId

Enumeration Value	Description
UNEXPECTED_UE_LOCATION	Unexpected UE location
UE_GEOFENCE	Geofencing

Enumeration ExceptionTrend

Table 7-31 ExceptionTrend

Enumeration Value	Description
IN_FENCE	Indicates the UE is within the defined geofence area.
OUT_FENCE	Indicates the UE is outside the defined geofence area.
UNKNOWN	The location of the UE is unknown.

Type NetworkAreaInfo

Table 7-32 NetworkAreaInfo

Attribute name	Data type	P	Cardinality	Description
ecgis	Array	O	0 to N	Is the list of E-UTRA cell identities.
ncgis	Array	O	0 to N	Is the list of NR cell identities
gRanNodeIds	Array	O	0 to N	Is the list of list of the NG-RAN nodes.
tais	Array	O	0 to N	Is the list of tracking area identities.

Type EventReportingRequirement

Table 7-33 EventReportingRequirement

Attribute name	Data type	P	Cardinality	Description
accuracy	Accuracy	O	0 to 1	Preferred level of accuracy of the analytics.
startTs	DateTime	O	0 to 1	UTC time indicating the start time of the observation period. The absence of this attribute means subscription at the present time.
endTs	DateTime	O	0 to 1	UTC time indicating the end time of the observation period. The absence of this attribute means subscription at the present time. If provided, it shall not be less than the start time.

Table 7-33 (Cont.) EventReportingRequirement

Attribute name	Data type	P	Cardinality	Description
sampRatio	SamplingRatio	O	0 to 1	Percentage of sampling (1 up to 100%) among impacted UEs.
maxSupiNbr	Uinteger		0 to 1	Represents the maximum number of SUPIs expected in an object. Applicable for the event(s) providing a list of SUPIs during the analyticis response.
maxObjectNbr	Uinteger		0 to 1	Maximum number of objects expected for an analytics report. It's only applicable for the event(s) which may provide more than one entries or objects during event notification.
timeAnaNeeded	DateTime		0 to 1	UTC time indicating the time when analytics information is needed.

Enumeration NotificationMethod

Table 7-34 NotificationMethod

Enumeration Value	Description
THRESHOLD	OCNWDAF subscription is notified when the defined threshold exceeds.

Enumeration Accuracy

Table 7-35 Accuracy

Enumeration Value	Description
LOW	Low accuracy
HIGH	High accuracy

Type SamplingRatio

Table 7-36 SamplingRatio

Name	Definition	Description
SamplingRatio	Integer	Unsigned integer indicating Sampling Ratio , expressed as percentage value from 1 up to 100.

8
Access OCNWDAF GUI Using CNC Console

This chapter describes how to configure different analytics parameters (global and service) and view analytics information in the Oracle Communications Networks Data Analytics Function (OCNWDAF) GUI. The OCNWDAF GUI is accessed using the CNC Console application. OCNWDAF provides a console interface using the highly secure GUI service, which allows you to use an interactive interface for performing various actions related to OCNWDAF services.

Support for Multicluster Deployment

CNC Console supports both single and multiple cluster deployments by facilitating OCNWDAF deployment in local and remote Kubernetes clusters. For more information about single and multiple cluster deployments, see *Oracle Communications Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide*.

A single instance of CNC Console can configure multiple clusters of OCNWDAF deployments, where each cluster has an agent console installation and a OCNWDAF installation.

CNC Console Interface

This section provides an overview of the Oracle Communications Cloud Native Configuration Console (CNCC), which includes an interface to configure the OCNWDAF features.

To configure the OCNWDAF services using the CNCC, log in to the CNCC application. To log into CNCC, update the hosts file available at the **C:\Windows\System32\drivers\etc location** when CNCC is hosted on a third party cloud native environment.

1. In the Windows system, open the hosts file in the notepad as an administrator and append the following set of lines at the end of the hosts file:

   ```
   <CNCC Node IP> cncc-iam-ingress-gateway.cncc.svc.cluster.local
   <CNCC Node IP> cncc-core-ingress-gateway.cncc.svc.cluster.local
   ```

   For example:

   ```
   10.75.212.88 cncc-iam-ingress-gateway.cncc.svc.cluster.local
   10.75.212.88 cncc-core-ingress-gateway.cncc.svc.cluster.local
   ```

   > **Note**
   >
   > The IP Address mentioned above may change when the deployment cluster changes.

2. Save and close the hosts file.
   Before logging into CNC Console, create a CNCC user name and password. Log in to the CNC Console application using these login credentials. For information on creating a CNC Console user and password, see *Oracle Communications Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide*.

8.1 OCNWDAF GUI Login

The OCNWDAF Graphical User Interface (GUI) can be accessed only after logging in to the CNC Console application. Before proceeding, ensure that the CNC Console is installed. For more information, see "Installing OCNWDAF GUI" section of *Oracle Communications Networks Data Analytics Function Installation and Fault Recovery Guide*.

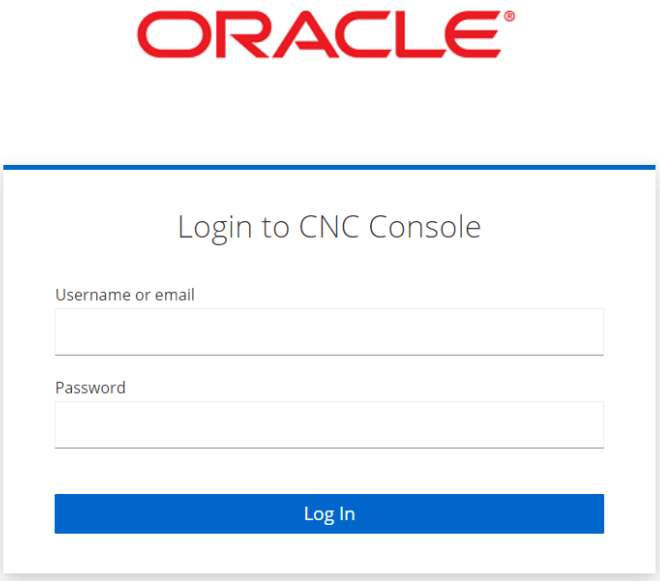
Before logging in to the CNC Console application, create a username and password. For more information about username creation, see "Configuring CNC Console IAM" section in *Cloud Native Configuration Console User Guide*.

CNC Console Log in

Following is the procedure to log into CNC Console:

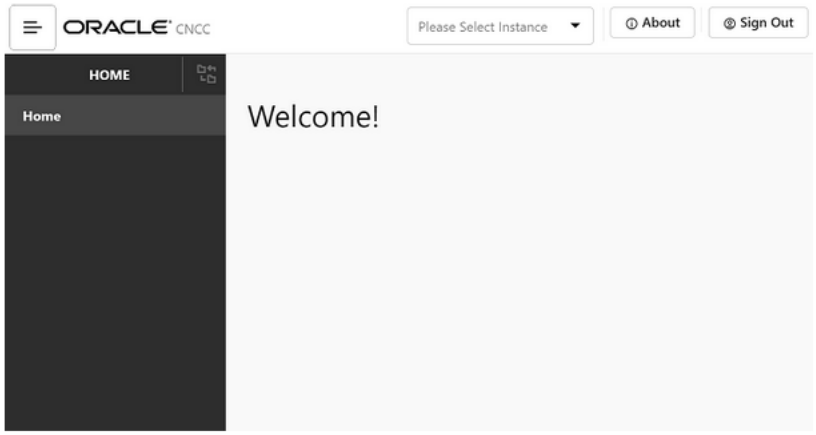
1. Open any web browser.
2. Enter the URL: http://<host name>:<port number>.
   where, host name is *cncc-iam-ingress-ip* and port number is *cncc-iam-ingressport*.
3. Enter valid login credentials.

Figure 8-1 CNC Console Login



4. Click **Log in**. The CNC Console interface is displayed.

Figure 8-2 CNC Console Interface



Select the required OCNWDAF instance from the **Please Select Instance** drop-down list. The left pane displays the selected network function.

On a new browser tab, the Machine Learning (ML) Model Selector page appears.

Figure 8-3 ML Model Selector

All GUI pages contain the following options:

- The **Logout** button to logout from the GUI.
- The **ML Model Selector** icon at the bottom of the page opens the **ML Model Selector** page.
- The **Slice Load Monitoring** icon at the bottom of the page opens the **Slice Load Monitoring** page.
- The **NF Load Monitoring** icon at the bottom of the page opens the **NF Load Monitoring** page.
- The **Geofence Monitoring** icon at the bottom of the page opens the **Geofence Monitoring** page.

- The **UE Mobility Monitoring** icon at the bottom of the page opens the **UE Mobility Monitoring** page.
- The **Monitoring** icon at the bottom of the page opens the **Monitoring** page.
- The **Configuration** icon at the bottom of the page opens the **Configuration** page.
- The **Capex Optimization** icon at the bottom of the page opens the **Capex Optimization** page.
- The **Dashboard** icon at the bottom of the page opens the **Dashboard** page.
- The **Alerts** icon at the bottom of the page opens the **Alerts** page.

The **ML Model Selector** page consists the following elements:

- The list of analytics for which the ML Models can be selected:
  - **ABNORMAL BEHAVIOUR**
  - **NETWORK PERFORMANCE**
  - **NF LOAD**
  - **UE MOBILITY**
  - **SLICE LOAD LEVEL**
  - **QOS SUSTAINABILITY**
  - **CAPEX**
- A brief of the **Description** selected analytics ID.
- The **Default** algorithm of the selected analytic.

To update the ML model for the OCNWDAF analytic IDs, see Machine Learning (ML) Model Selector.

8.2 Machine Learning (ML) Model Selector

Use the **ML Model Selector** page to update or select the Machine Learning (ML) model for the OCNWDAF analytic IDs. It contains the following elements:

- The list of analytics IDs for which the ML algorithms can be selected are:
  - **ABNORMAL BEHAVIOUR**
  - **NETWORK PERFORMANCE**
  - **NF LOAD**
  - **UE MOBILITY**
  - **SLICE LOAD LEVEL**
  - **QOS SUSTAINABILITY**
  - **CAPEX**
- A brief of the **Description** analytic ID.
- The **Default** algorithm of the selected analytic ID. The **Lock** icon is used to select a new algorithm from the drop-down list.

Follow the steps below to update the ML algorithm, run experiments, and view historical experiments for the OCNWDAF analytic IDs:

1. Click the analytic ID for which you want to update the ML algorithm. The following options appear below the selected Analytic ID:
   - **Model Config**
   - **Experiments**
   - **Historical**

   For example:

Figure 8-4 ML Model Selector for an Analytic ID

2. The **Model Config** option displays a brief **Description** of the analytic ID and the **Default** ML algorithm. Click **Lock** icon to select a new algorithm from the drop-down list. Listed below are the algorithm options for each Analytic ID:

Table 8-1 ML Algorithm

Analytic ID	Algorithm Options
ABNORMAL BEHAVIOUR	• **Random Forest Classifier**. • **Support Vector Classifier** (this is the default algorithm). • **Gradient Boosting Classifier** • **Logistic Regression**
NETWORK PERFORMANCE	• **Random Forest Regressor** (this is the default algorithm). • **Decision Tree Regressor** • **Linear Regression**
NF LOAD	• **Multi-layer Perceptron Regressor**. • **Random Forest Regressor** • **Gradient Boosting Regressor** • **Decision Tree Regressor** • **SARIMAX** (this is the default algorithm). Provide the following **Model Tuning Parameter**: – **Enter Moving Average Value - MA(q)** – **Enter Auto Regressive Value - AR(p)** Click **Update Model**.

Table 8-1 (Cont.) ML Algorithm

Analytic ID	Algorithm Options
UE MOBILITY	• **Long Short Term Memory Network** (this is the default algorithm). • **Feed Forward Neural Network** • **Recurrent Neural Network**
SLICE LOAD LEVEL	• **Linear Regression**, this is the default algorithm. • **Random Forest Regressor** • **Gradient Boosting Regressor** • **K Neighbors Regressor**
QOS SUSTAINABILITY	• **Decision Tree Regressor** (this is the default algorithm). • **Random Forest Regressor** • **K Neighbors Regressor**
CAPEX	• **Decision Tree Regressor** • **Random Forest Regressor** (this is the default algorithm).

Select the algorithm, a pop-up window appears to confirm the change in the "Default Algorithm". Click **Yes** to confirm the change, click **Cancel** to discard the change.

A **Success** message is displayed after the algorithm is successfully changed.

The selected algorithm will now be used to train a model for the analytics category.

3. Click **Experiments** option for the analytics ID to run experiments on the selected algorithm.
   - Click the check box to select the algorithm.

> **Note**
>
> User can select multiple algorithms simultaneously.

The following algorithms are available for each analytic ID:

Table 8-2 Select Algorithm

Analytic ID	Algorithm Options
ABNORMAL BEHAVIOUR	– **Gradient Boosting Classifier** – **Random Forest Classifier** – **Logistic Regression** – **Support Vector Classifier**
NETWORK PERFORMANCE	– **Random Forest Regressor** – **Decision Tree Regressor** – **Linear Regression**
NF LOAD	– **Gradient Boosting Regressor** – **Decision Tree Regressor** – **Multi-layer Perceptron Regressor** – **Random Forest Regressor**

Table 8-2 (Cont.) Select Algorithm

Analytic ID	Algorithm Options
UE MOBILITY	– Long Short Term Memory Network – Recurrent Neural Network – Feed Forward Neural Network
SLICE LOAD LEVEL	– Gradient Boosting Regressor – Random Forest Regressor – Linear Regression – K Neighbors Regressor
QOS SUSTAINABILITY	– K Neighbors Regressor – Decision Tree Regressor – Random Forest Regressor
CAPEX	– Random Forest Regressor – Decision Tree Regressor

- Provide an **Experiment Name**.
- Click **Run Experiment**, to run experiments with the selected algorithm(s).
- A success message is displayed on the screen with the Experiment ID.

4. Click **Historical** to see information about the experiments previously run for the analytics ID. The list of experiments with the following details is displayed:

Figure 8-5 Historical Data

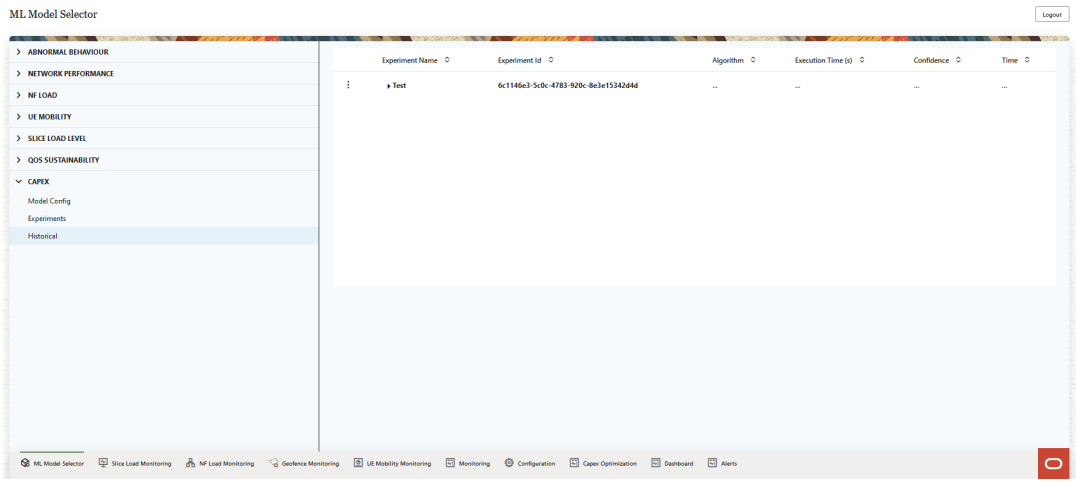


Table 8-3 Historical Data

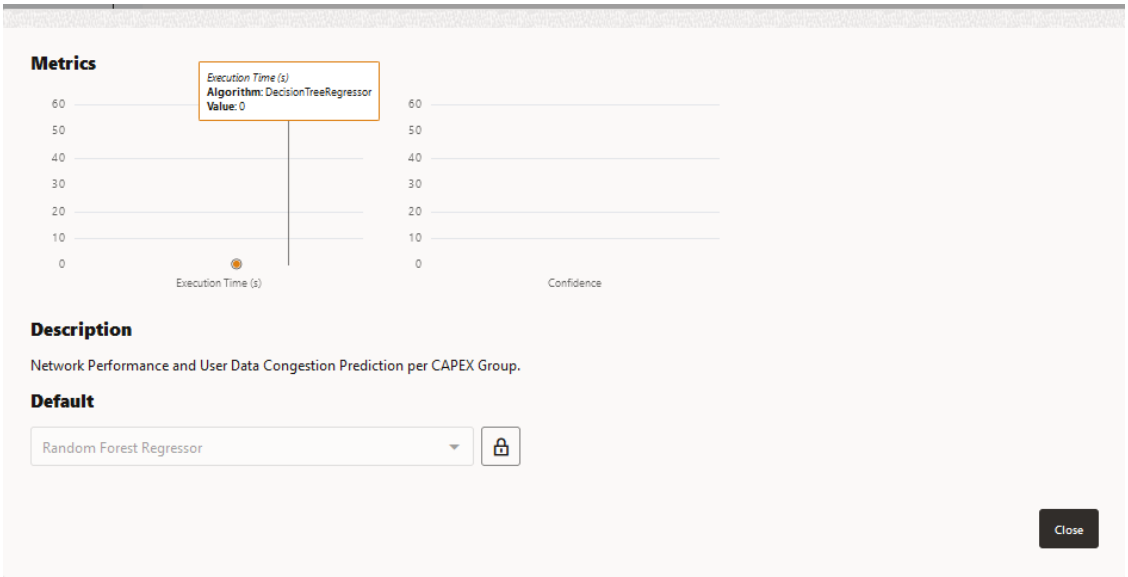
Parameter	Description
Experiment Name	The experiment name provided by the user.
Experiment ID	The unique identifier of the experiment.
Algorithm	The algorithm used for the experiment.
Execution Time (s)	The time duration for which the experiment was conducted.
Confidence	The confidence value of the experiment.

Table 8-3 (Cont.) Historical Data

Parameter	Description
Time	The date and time when the experiment was conducted.
The **Vertical Ellipses** icon	Click this icon to view metrics for the experiment. Click **View Metrics**, a pop-up appears to display the metrics information (for example, Figure 8-6)

Sample Metrics screen:

Figure 8-6 Metrics



After reviewing the results, you can change the **Default** algorithm. Click the **Lock** icon and then select an algorithm from the drop-down list.

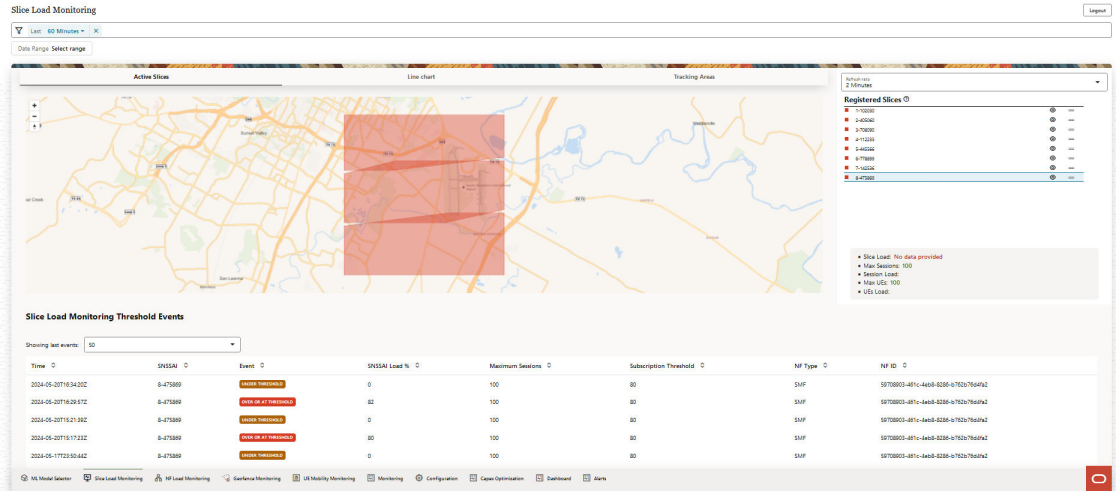
Select the algorithm, a pop-up window appears to confirm the change in the "Default Algorithm". Click **Yes** to confirm the change, click **Cancel** to discard the change.

A **Success** message is displayed after the algorithm is successfully changed.

8.3 Slice Load Monitoring

The **Slice Load Monitoring** screen displays different visualization styles of slice data.

Figure 8-7 Slice Load Monitoring



A Filter bar to filter the slice load information based on **Date Range** (click **Select range** to set the dates) or the option **Last** (click drop-down to select 3 Minutes, 5 Minutes, 15 Minutes, 30 Minutes, 60 minutes or 120 minutes) to filter based on the minutes elapsed.

The page includes three tabs **Active Slices**, **Line Chart**, and **Tracking Areas**.

All tabs display the following **Slice Load Monitoring Threshold Events** information:

- The user can select the number of previous events to be displayed. Select the number of events using the **Showing last events** drop down list. The allowed values are **5**, **10**, **20**, and **50**.
- A list of slices with the following information is displayed:
  - **Time**: The timestamp of the slice.
  - **SNSSAI**: The S-NSSAI of the slice.
  - **Event**: Displays if the event is "Under Threshold" or "Over of At Threshold".
  - **SNSSAI Load %**: Displays the percentage of load on the S-NSSAI.
  - **Maximum Sessions**: Displays the number of maximum sessions.
  - **Subscription Threshold**: Displays the configured subscription threshold.
  - **NF Type**: Displays the NF Type. For example AMF, SMF, and so on.
  - **NF ID**: Displays the value of the NF Id.

  Use the **Arrow** icon provided for each of the above parameters to list the values in ascending order.

Active Slices

Configure the **Refresh rate** of the page from the drop-down list. The allowed values are **1 Minute**, **2 Minutes**, **3 Minutes**, **5 Minutes**, and **10 Minutes**.

The **Active Slices** tab displays the **Registered Slices** in the region. The slices are color coded. Click on any of the listed **Registered Slice**, the following information about the slice is displayed on the right side of the screen:

- **Slice Load**: Displayed as a percentage (%) value.
- **Max Sessions**: Displays the maximum number of sessions in the slice.

- **Session Load**: Displays the session's load information in the slice.
- **Max UEs**: Displays the maximum number of UEs in the slice.
- **UEs Load**: Displays the UEs load information.

The **Registered Slices** are also displayed on the map view of the page. To view or block the display of the slice on the map click the **Eye** icon provided for each **Registered Slice** displayed in the list. You can change the order in which the slices are drawn in the map view. Reorder the list of **Registered Slice** displayed on the screen, drag the slice to reorder the list. Slices in the map view are redrawn according to the order of the **Registered Slice**. This option allows active slices hidden below to be displayed on top.

You can hover the mouse over the map, use the **+** and **-** icons to adjust the zoom, and drag and adjust the map view as required.

This tab also displays the **Slice Load Monitoring Threshold Events** information

Line Chart

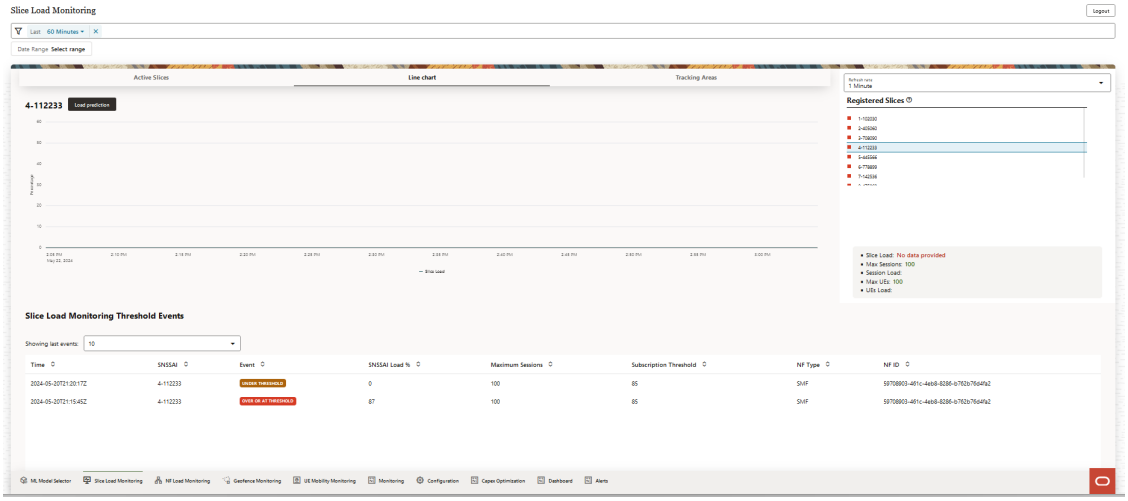
Configure the **Refresh rate** of the page from the drop-down list. The allowed values are **1 Minute**, **2 Minutes**, **3 Minutes**, **5 Minutes**, and **10 Minutes**.

The **Line Chart** tab displays the Line Charts for the **Registered Slice** in the region.

Click **Load Prediction** to display the predictions for the selected slice.

Hover on the line chart to view the **Series Slice Load** information, **Date**, and **Load**.

Figure 8-8 Slice Load Graph



The **Registered Slices** are also listed on the right-side of the page. Click on any **Registered Slice**, the following information about the slice is displayed on the right side of the screen:

- **Slice Load**: Displayed as a percentage (%) value.
- **Max Sessions**: Displays the maximum number of sessions in the slice.
- **Session Load**: Displays the session's load information in the slice.
- **Max UEs**: Displays the maximum number of UEs in the slice.
- **UEs Load**: Displays the UEs load information.

This tab also displays the **Slice Load Monitoring Threshold Events** information

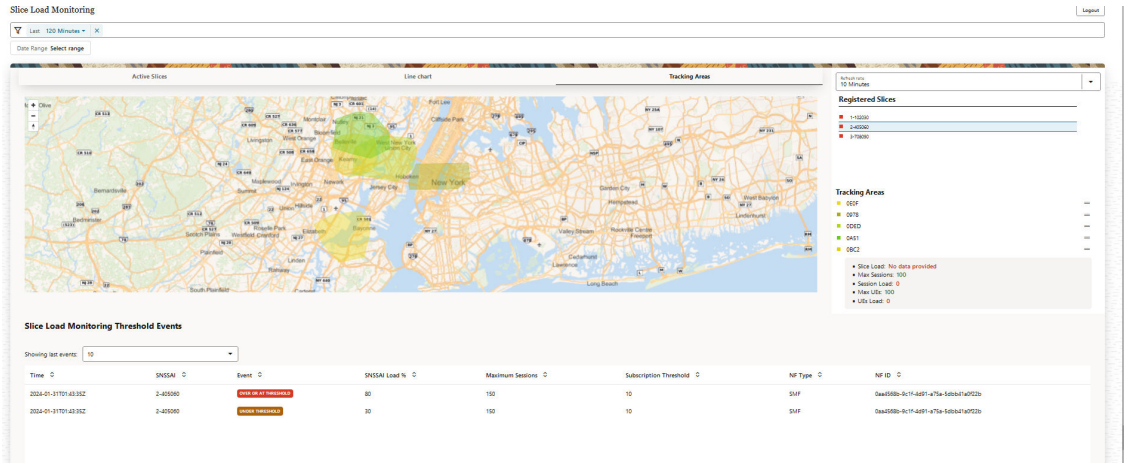
Tracking Areas

Configure the **Refresh rate** of the page from the drop-down list. The allowed values are **1 Minute**, **2 Minutes**, **3 Minutes**, **5 Minutes**, and **10 Minutes**.

The **Tracking Areas** tab displays tracking areas in the **Registered Slices** of the region. The slices and tracking areas are color coded. The **Registered Slices** are listed on the right-side of the page. Click on any **Registered Slice**, the following information about the slice is displayed on the right side of the screen:

- List of **Tracking Areas** in the slice. The Tracking Areas have an Id and are color coded.
- **Slice Load**: Displayed as a percentage (%) value.
- **Max Sessions**: Displays the maximum number of sessions in the slice.
- **Session Load**: Displays the session's load information in the slice.
- **Max UEs**: Displays the maximum number of UEs in the slice.
- **UEs Load**: Displays the UEs load information.

Figure 8-9 Tracking Areas



The **Tracking Areas** are also displayed on the map view of the page. You can change the order in which the tracking areas are drawn in the map view. Reorder the list of **Tracking Areas** displayed on the screen, drag the tracking area to reorder the list. Tracking areas in the map view are redrawn according to the order of the **Tracking Areas**, this option allows tracking areas hidden below to be displayed on top.

You can hover the mouse over the map, use the **+** and **-** icons to adjust the zoom, and drag and adjust the map view as required.

This tab also displays the **Slice Load Monitoring Threshold Events** information

8.4 NF Load Dashboard

The **NF Load Dashboard** screen displays the NF Load information, that includes NF instances, NF load level as peak and average load values. It also displays the NF Load Monitoring Threshold Events information. Click on the **Graph** icon on the left side of the screen to view graphs of **Round Trip Time**, **Observed Transactions Per Second**, **Error Count** (only for UDM), and **NF Load**.

Figure 8-10 NF Load Monitoring

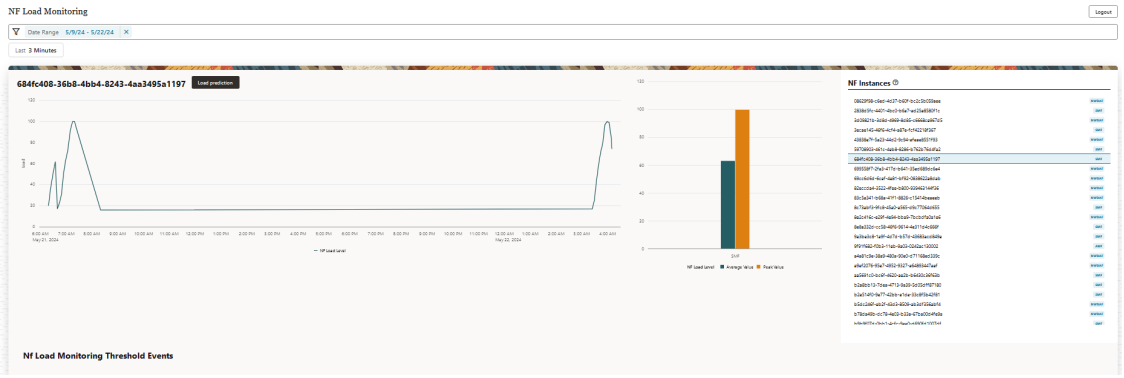
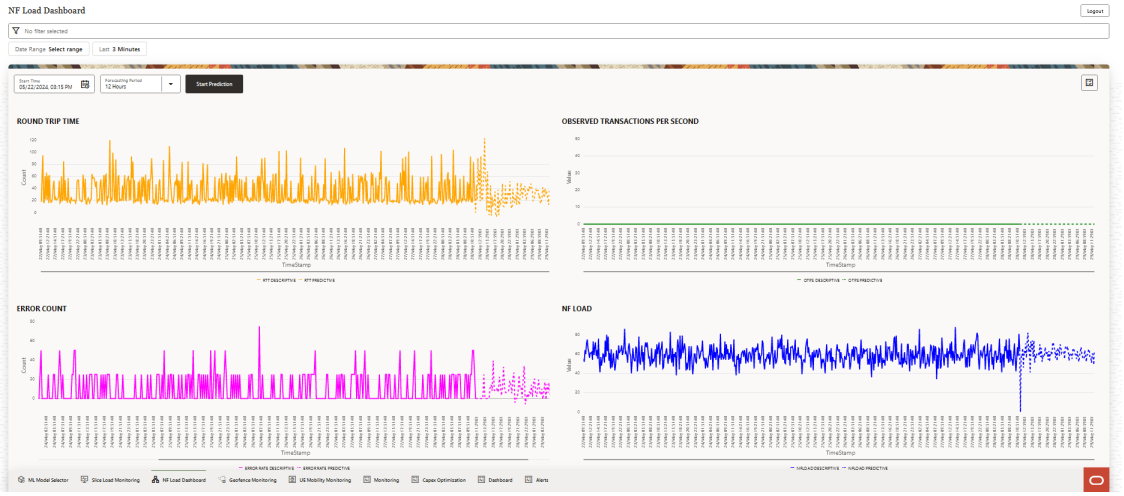


Figure 8-11 NF Load Monitoring Graphs



A Filter bar to filter the NF load information based on **Date Range** (click **Select range** to set the dates), and the option **Last** (click drop-down to select 3 Minutes, 5 Minutes, 15 Minutes, 30 Minutes, 60 minutes or 120 minutes) to filter based on the minutes elapsed. The **Date Range** can be set to a future date to obtain Predictive Analytics information.

Select the parameters, **Start Time** and **Forecasting Period** and click **Start Prediction** to obtain NF Load predictions. The **Start Time** includes date and time information and the **Forecasting Period** can be 12 Hours, 24 Hours, 36 Hours, or 48 Hours.

The **NF Instances** are listed on the right side of the screen, select the NF instance to view the load levels for that NF.

The **NF Load Monitoring** screen provides a graphical display of load levels for each NF:

- **NF Load Level**, it includes the following:
  - A graphical representation of the NF load level and load values with time stamp.
  - A graphical representation of the **Peak Value**.
  - A graphical representation of the **Average Value**.

Hover on the bar graph to view **Peak Load Value**, **NF Instance Id**, **NF Type**, and **NF Load**.

Hover on the line graph to view **NF load Level**, **Date**, and **Load**.

Use the **Showing Last Events** drop-down list to select the number of previous NF load level events to be displayed on the screen.

A list of NFs with the following information is displayed:

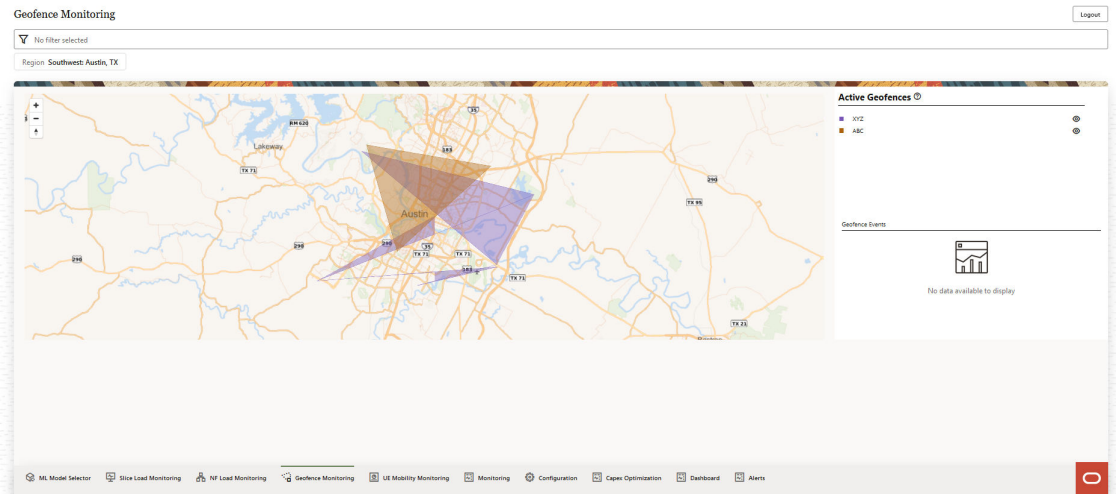
- **Time**: The timestamp of the NF.
- **NF Type**: The NF type such as AMF, SMF, or NWDAF and so on.
- **NF Instance Id**: The NF instance identifier.
- **Average Load Level %**: Displays the average load level on an NF (in percentage).
- **Peak Load Level %**: Displays the peak load level of an NF (in percentage).
- **Crossing Type**: Indicates the crossing type that is "ASCENDING", DESCENDING", or "CROSSED".

Use the **Arrow** icon provided for each of the above parameters to list the values in ascending order.

8.5 Geofence Monitoring

The **Geofence Monitoring** page displays the Active Geofences and the Geofence Events.

Figure 8-12 Geofence Monitoring



A Filter bar to filter the Geofence information based on **Region** (click region drop-down list to select the region). The filter selection can be refreshed by clicking on the Refresh icon.

The **Geofence Monitoring** screen displays the **Active Geofences** in the region. The geofences are color coded. The **Active Geofences** are also listed on the right-side of the page. Click the **Eye** icon to view or block the display of the geofence on the map.

The **Geofence Events** are listed on the right-side of the page. For each geofence event the following information is displayed:

- **Supi**: Indicates the SUPIs of the UEs.
- **Event Type**: Is displayed as "IN FENCE" when the UE is within the defined geofence area, or "OUT OF_FENCE" if the UE is outside the defined geofence area.

- Click the **Target** icon to determine if the UE is within or outside the geofence area. The icon changes to the **Location** icon. Click the **Location** icon determine the location of the UE on the map.

Use the **Arrow** icon provided for each of the above parameters to list the values in ascending order.

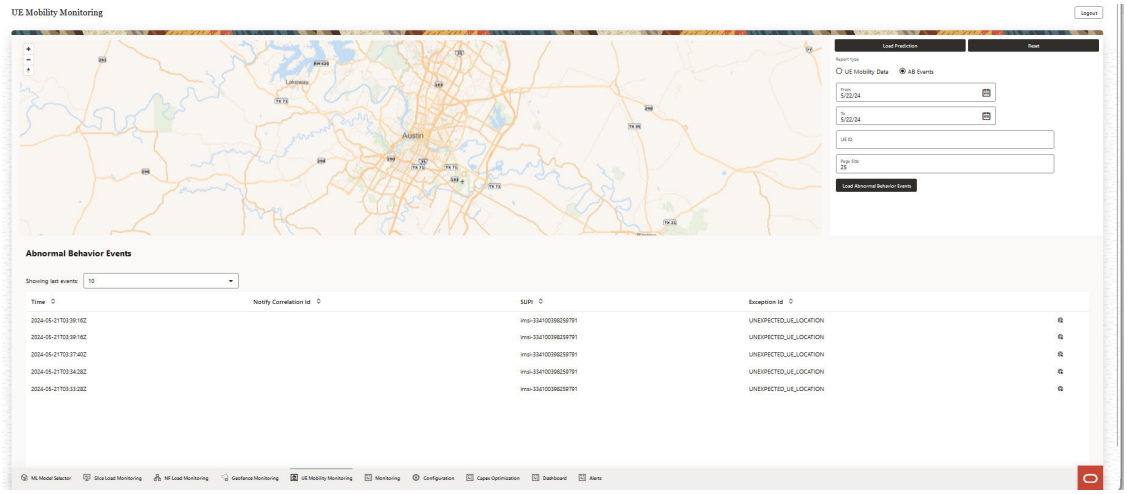
To add, update, or delete a geofence see, Geofence Settings on the **Configuration** page.

8.6 UE Mobility Monitoring

The **UE Mobility Monitoring** screen displays the UE Mobility Data and Abnormal Behavior (AB) Events information.

To obtain UE Mobility Data, select the radio button **UE Mobility Data** or select the radio button **AB Events** to obtain information on the abnormal events.

Figure 8-13 UE Mobility Monitoring



UE Mobility Data

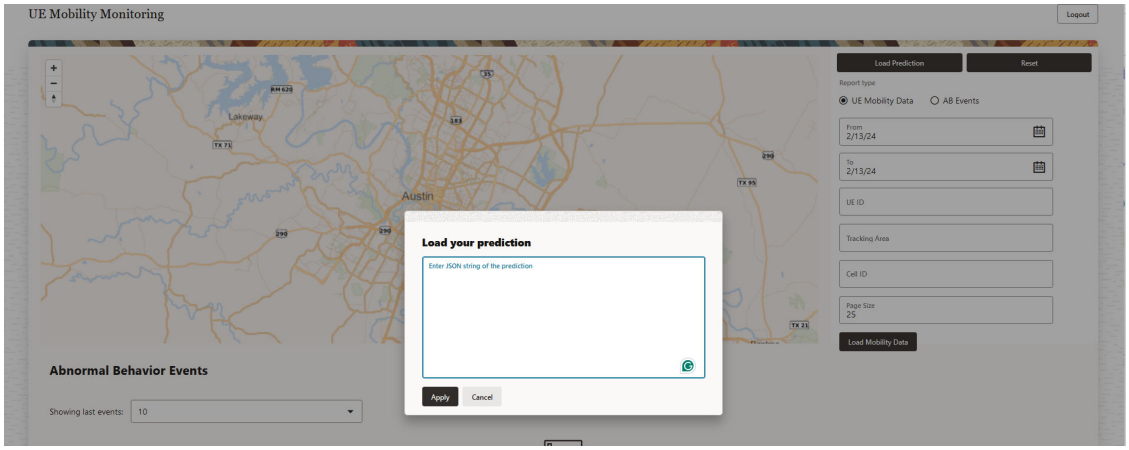
Provide the following information to obtain UE Mobility Data :

- **From** date, click on the **Calender** icon to select the start date.
- **To** date, click on the **Calender** icon to select the end date.
- **UE ID**
- **Tracking Area**
- **Cell ID**
- **Page Size**

Click **Load Mobility Data**.

To obtain load prediction information click **Load Prediction**.

Figure 8-14 Load Prediction



Enter the JSON string of the prediction in the text box. Click **Apply**. To discard the changes, click **Cancel**.

Click **Reset** to discard the existing values.

AB Events

Provide the following information to obtain information on abnormal events:

- **From** date, click on the **Calender** icon to select the start date.
- **To** date, click on the **Calender** icon to select the end date.
- **UE ID**
- **Page Size**

Click **Load Abnormal Behavior Events**.

To obtain load prediction information click **Load Prediction**.

Enter the JSON string of the prediction in the text box. Click **Apply**. To discard the changes, click **Cancel**.

Click **Reset** to discard the existing values.

This page lists **Abnormal Behavior Events** information:

- The user can select the number of previous events to be displayed. Select the number of events using the **Showing last events** drop down list.
- A abnormal events with the following information is displayed:
  - **Time**
  - **Notify Correlation Id**
  - **SUPI**
  - **Exception ID**

  Click the **Target** icon listed against the abnormal event, the event location is displayed on the map. The icon changes to the **Location** icon.

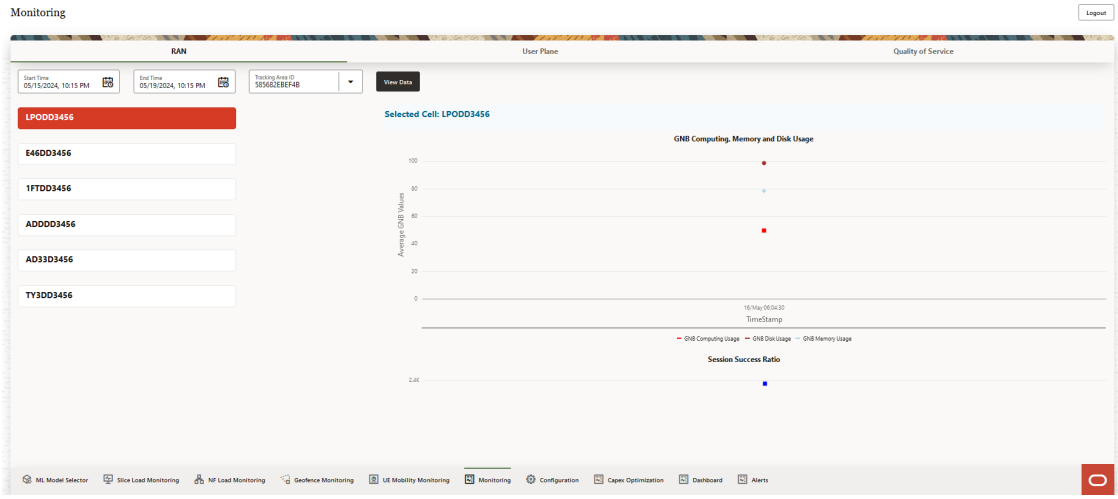
  Use the **Arrow** icon provided for each of the above parameters to list the values in ascending order.

8.7 Monitoring

The **Monitoring** page displays the following analytics information:

- Network Performance Analytics
- User Data Congestion Analytics
- QoS Sustainability Analytics

Figure 8-15 Monitoring



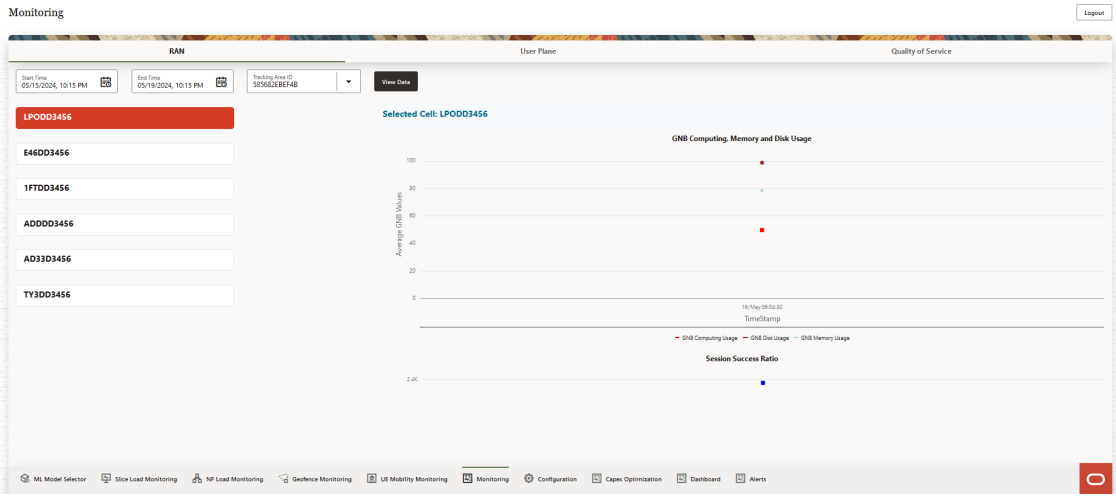
The page includes of three tabs **RAN**, **User Plane**, and **Quality of Service**.

The **RAN** tab displays information related to Network Performance Analytics,the **User Plane** tab displays the User Data Congestion Analytics, and the **Quality of Service** tab displays the QoS Sustainability Analytics reports and trends.

RAN

Click **RAN**, to see Network Performance Analytics information.

Figure 8-16 RAN



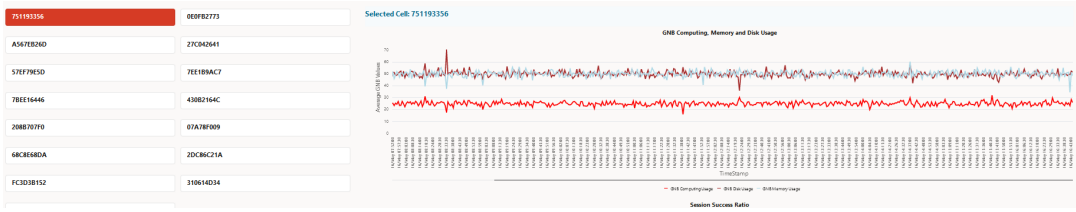
Follow the steps to view information for the selected tracking ID and time interval:

1. Select the **Start Time** and **End Time**.
2. Use the **Tracking Area ID** drop-down list to select the tracking area for which the analytics information is required.
3. Click **View Data**.

The cells available in the selected **Tracking Area ID** within the selected time interval are displayed on the screen. Click any cell to view the graphic visualizations of resource usage related to the following fields are displayed on the screen:

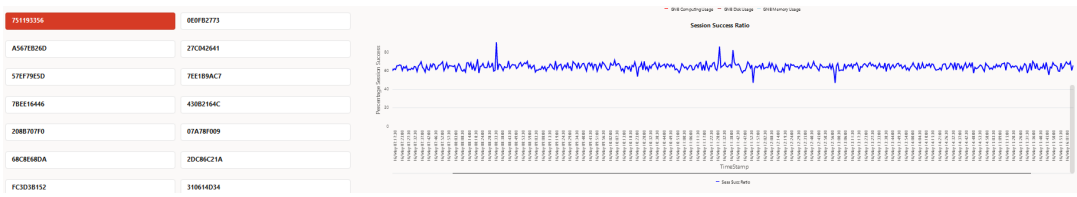
- **GNB Computing, Memory, and Disk Usage**
  For example:

Figure 8-17 GNB Computing, Memory, and Disk Usage



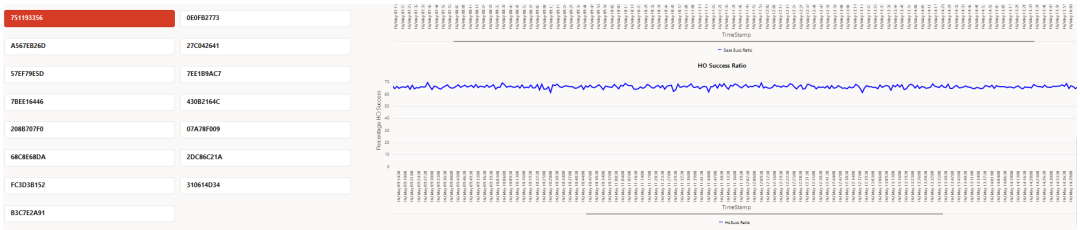
- **Session Success Ratio**
  For example:

Figure 8-18 Session Success Ratio



- **HO Success Ratio**
  For example:

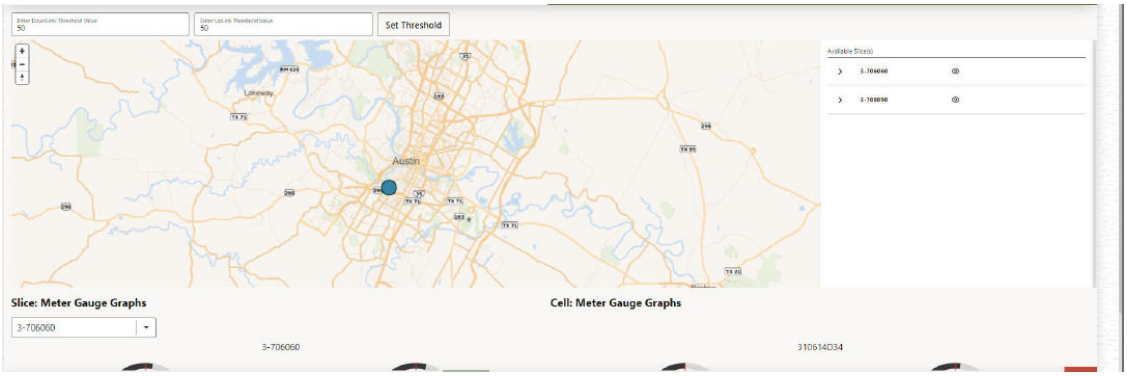
Figure 8-19 HO Success Ratio



User Plane

Click **User Plane** to see User Data Congestion Analytics information.

Figure 8-20 User Plane



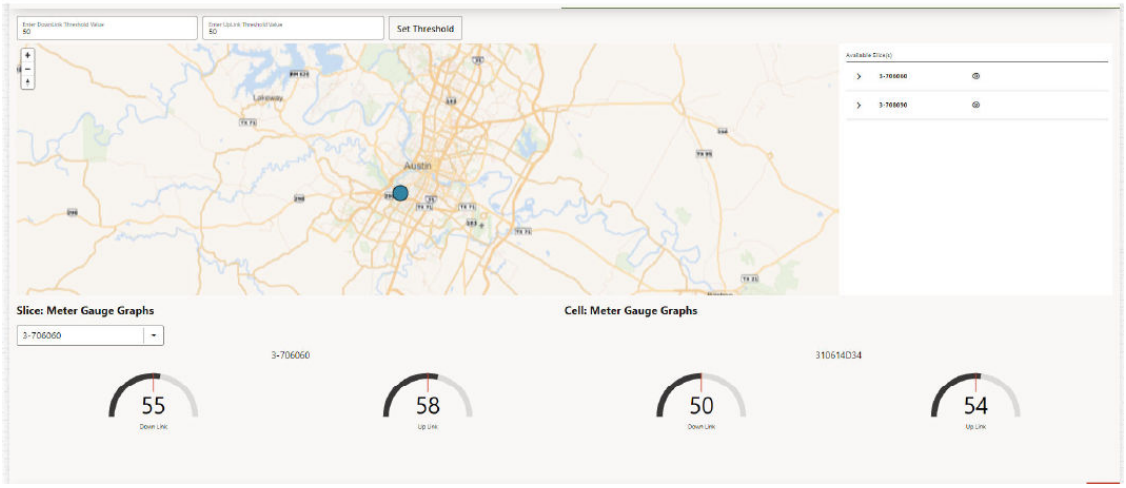
The list **Available Slice(s)** and **Cells** are displayed on the right side of the screen. To view or block the display of the slice on the map click **Eye** icon. Use the **Arrow** icon to view the list of cells in that slice. Click any **Cell** on the map, the following graphic visualizations are displayed on the screen:

- **Slice:Meter Gauge Graphs**: Uplink and downlink values are displayed.
- **Cell:Meter Gauge Graphs**: Uplink and downlink values are displayed.

To view the downlink and uplink throughput per slice use the dropdown list **Slice: Meter Gauge Graphs** to select the slice. The Meter Gauges for uplink and downlink throughput for the selected slice is displayed on the screen.

For example:

Figure 8-21 User Data Congestion



Perform the steps to view information for the specified uplink and downlink threshold values:

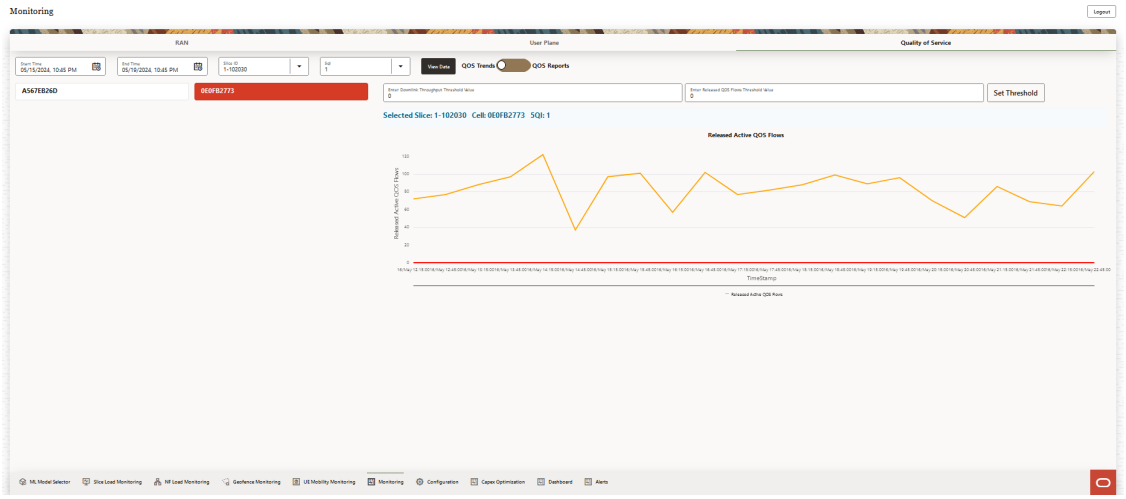
1. To **Set Threshold**, follow the steps below:
   a. Provide a threshold value in the **Enter DownLink Threshold Value** text-box. The default value and the permitted maximum value is 100.
   b. Provide a threshold value in the **Enter UpLink Threshold Value** text-box. The default value and the permitted maximum value is 100.
   c. Click **Set Threshold**.

The list of **Available Slice(s)** within the specified thresholds is displayed on the screen.

Quality of Service

Click **Quality of Service**, to see QoS Sustainability Analytics information such as QoS trends and reports.

Figure 8-22 Quality of Service



Use the toggle switch to select viewing either the **QOS Trends** or the **QOS Reports**.

Provide **Start Time**, **End Time**, **Slice ID**, and **5qi** (from the drop-down list of available values of "1" up to "8"). The cells in the slice are displayed on the screen. Click **View Data** to view graphic visualization of Released Active QoS Flows.

Click any **Cell** icon to view the graphic visualization of Released Active QoS Flows for that cell.

You can set the threshold values, **Enter Downlink Throughput Threshold Value** (in Kbps) and **Enter Released QOS Flows Threshold Value**, click **Set Threshold**.

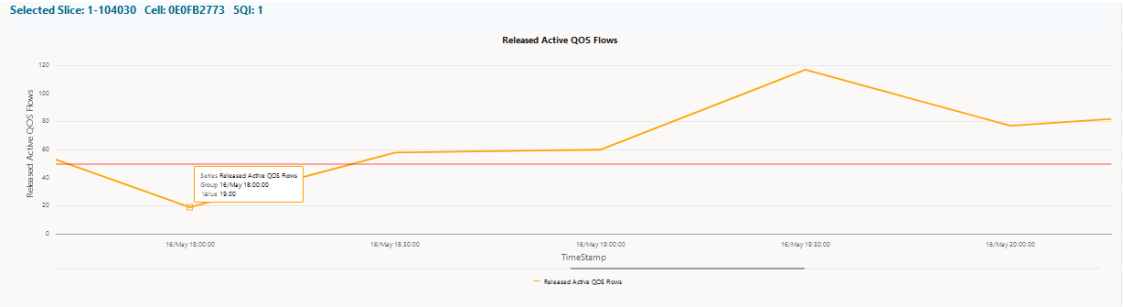
QOS Trends

Click any **Cell** icon. The **Released Active QoS Flows** with timestamp (date and time) is displayed on the screen.

> **Note**
>
> Use the zoom and scroll function on the graphs for a precise view of the data.

For example:

Figure 8-23 QoS Trends

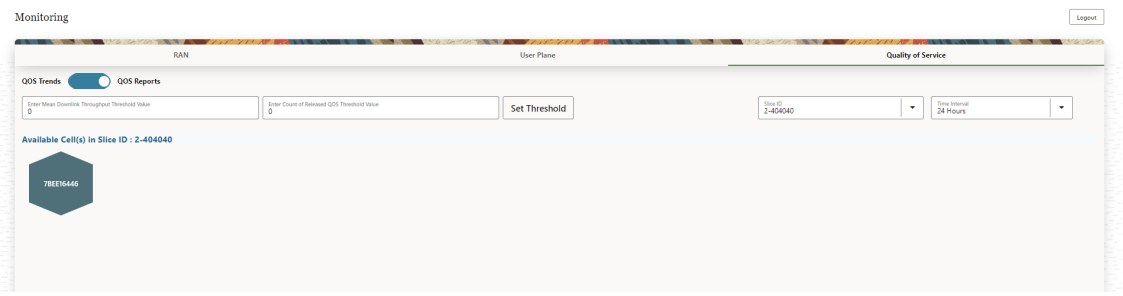


QOS Reports

Use the toggle switch, select **QOS Reports**. The cells in the selected slice are displayed on the screen.

For example:

Figure 8-24 QoS Reports

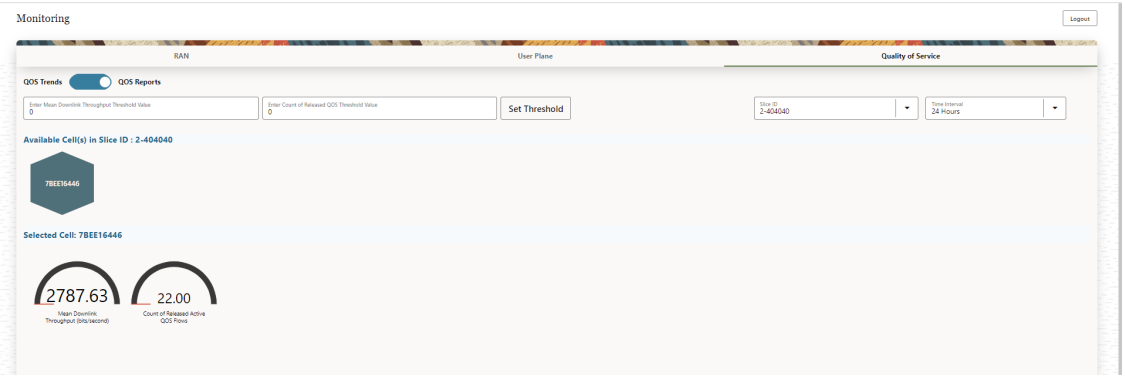


Click any **Cell** icon. The following graphic visualizations are displayed on the screen:

- A meter gauge graph displaying the **Mean Downlink Throughput (bits/second)** for the selected cell is displayed on the screen.
- A meter gauge graph displaying the **Count of Released Active QOS Flows** for the selected cell is displayed on the screen.

For example:

Figure 8-25 QoS Reports



Follow the steps to view information for a selected Slice ID, threshold, and time interval:

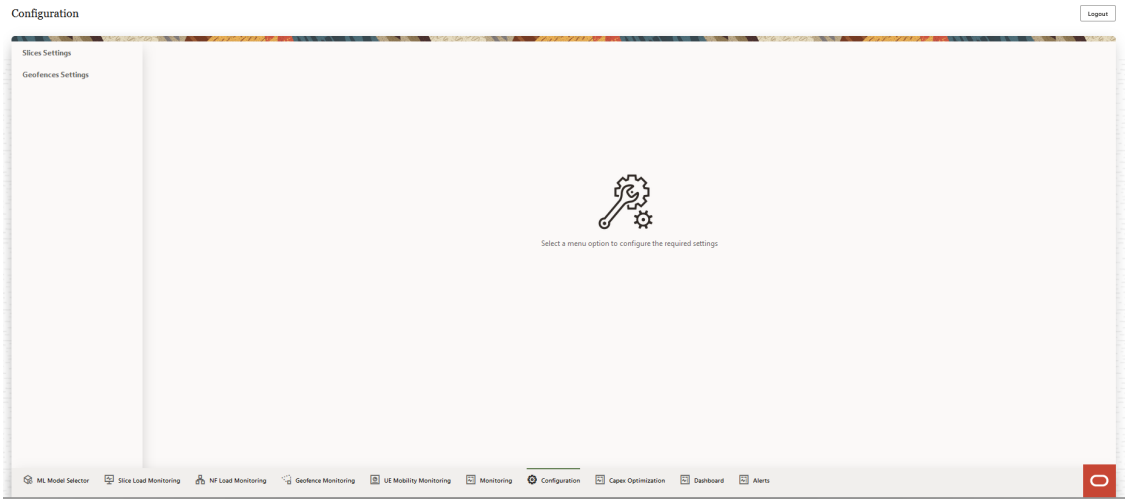
1. To **Set Threshold**, follow the steps below:
   - Provide a threshold value in the **Enter Downlink Throughput Threshold Value** text-box. For **QOS Trends**, enter a valid value in the range 0 up to the maximum permitted value. The maximum permitted value will be displayed when you click on the text-box. For **QOS Reports** enter a valid value in the range 0 up to the maximum permitted value. The maximum permitted value will be displayed when you click on the text-box.
   - Provide a threshold value in the **Enter Released QOS Flows Threshold Value** text-box. For **QOS Trends** the default value is 0 and the permitted range of values is 0 up to the maximum permitted value. The maximum permitted value will be displayed when you click on the text-box. For **QOS Reports** the default value is 0 and the permitted range of values is 0 up to the maximum permitted value. The maximum permitted value will be displayed when you click on the text-box.
   - Click **Set Threshold**.
2. Use the **Slice ID** drop-down list to select the Slice for which the analytics information is required.
3. Use the **Time Interval** drop-down list to select the interval for which the analytics information is required. The available interval options are **24 Hours**, **48 Hours**, **72 Hours**, and **96 Hours**.

The cells available in the selected **Slice ID** within the selected **Time Interval** and threshold values are displayed on the screen. Click on any cell to view the graphic visualizations of various parameters related to that cell.

8.8 Configuration

The **Configuration** page displays options to configure **Slices Settings** and **Geofences Settings**.

Figure 8-26 Configuration



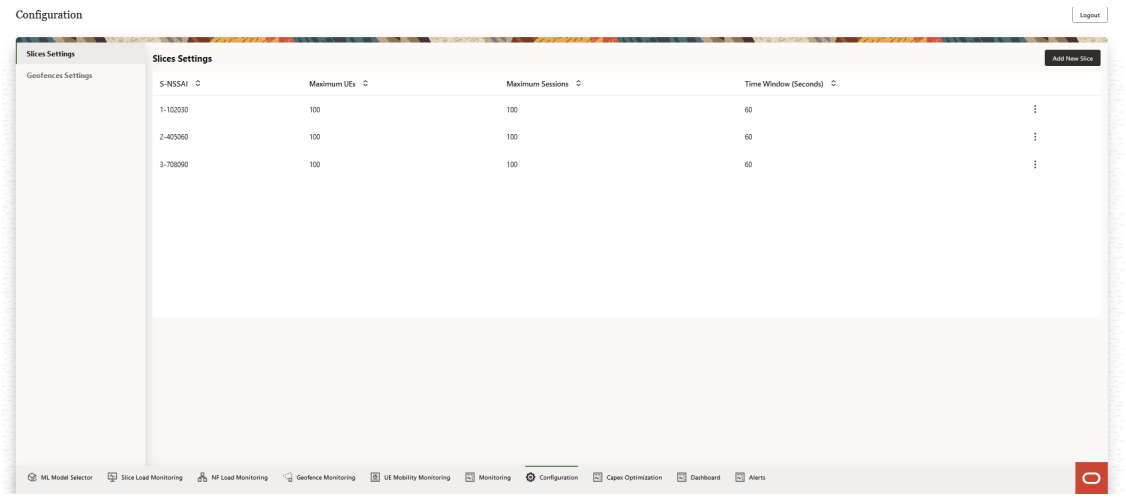
The user can perform the following actions through the **Configuration** page:

- Access the **Slice Settings** page.
- Access the **Geofence Settings** page.

8.8.1 Slices Settings

The **Slices Settings** page provides an option to **Add New Slice** and view the **Slice Settings** of all the configured slices.

Figure 8-27 Slice Settings



The user can perform the following actions on the **Slices Settings** page:

- **Add New Slice**
- View the configured slices and the slice parameters:

- **S-NSSAI**
- **Maximum UEs**
- **Maximum Sessions**
- **Time Window (Seconds)**

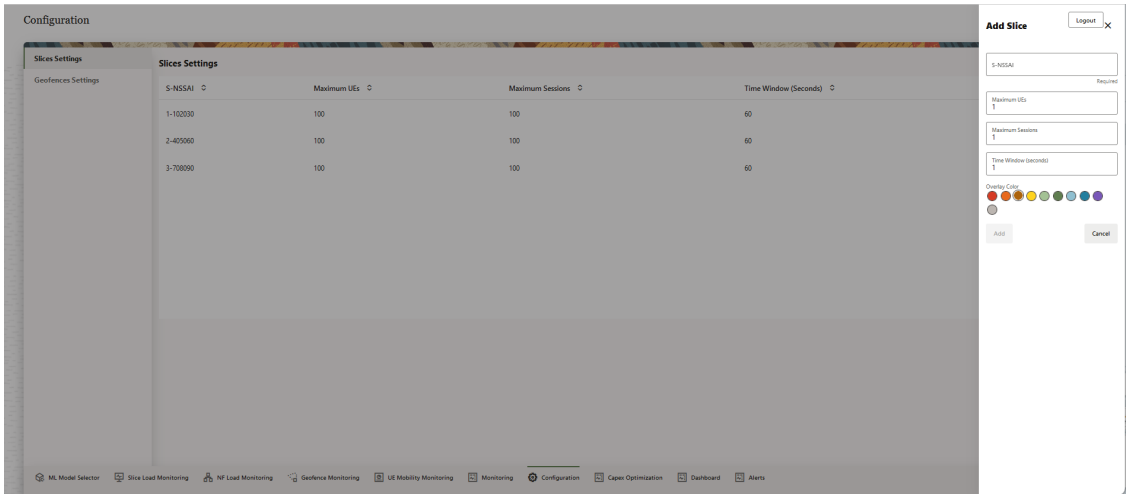
Use the **Arrow** icon provided for each of the above parameters to list the values in ascending order.

- Click the vertical **Ellipses** icon to edit a slice. The **Edit Value** option appears in a pop-up window.
- Click the vertical **Ellipses** icon to delete a slice. The **Delete** option appears in a pop-up window.

8.8.1.1 Add New Slice

To add a new slice, click **Add New Slice** on the **Slices Settings** screen. The **Add Slice** form appears on the right side of the screen:

Figure 8-28 Add Slice



Provide the following information to create a new slice:

Table 8-4 Add Slice

Parameter	Type	Description
S-NSSAI	String	The S-NSSAI is the network slice identifier. This parameter is mandatory.
Maximum UEs	Integer	The maximum number of user equipments allowed in the slice.
Maximum Sessions	Integer	The maximum number of sessions allowed in the slice.
Time Window (seconds)	Seconds	Threshold detection window time. Default: 5 minutes.

Table 8-4 (Cont.) Add Slice

Parameter	Type	Description
Overlay Color	Color	Select a display color for the slice.

Click **Add** to create a new slice. The new slice is listed in the **Slices Settings** screen.

To discard the changes click **Cancel**.

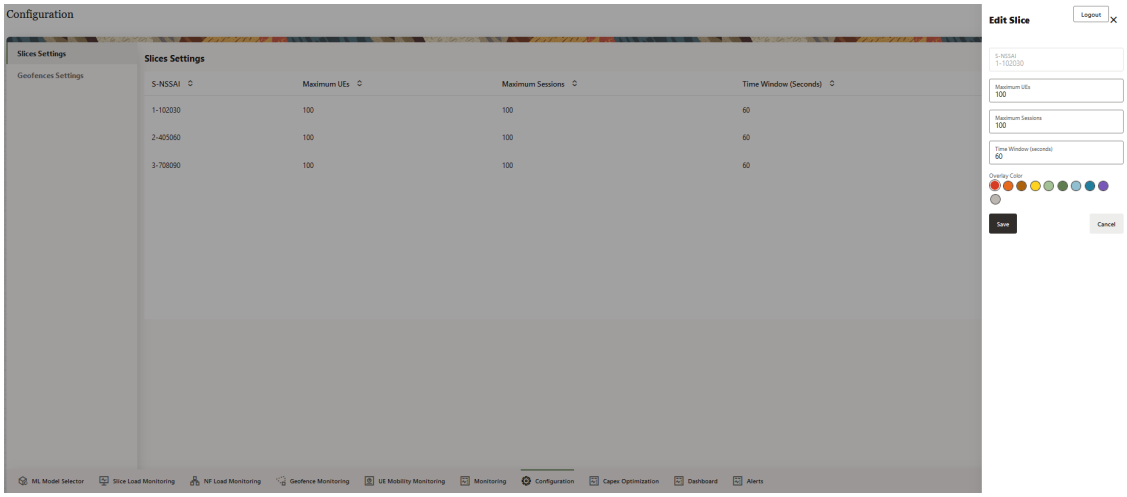
8.8.1.2 Edit Slice

In the **Slices Settings** screen, click the vertical **Ellipses** icon on the right side of the slice to be edited.

Click the **Edit Value** option that appears in a pop-up window.

The **Edit Slice** form appears on the right side of the screen.

Figure 8-29 Edit Slice



Note: The **S-NSSAI** of the slice cannot be modified.

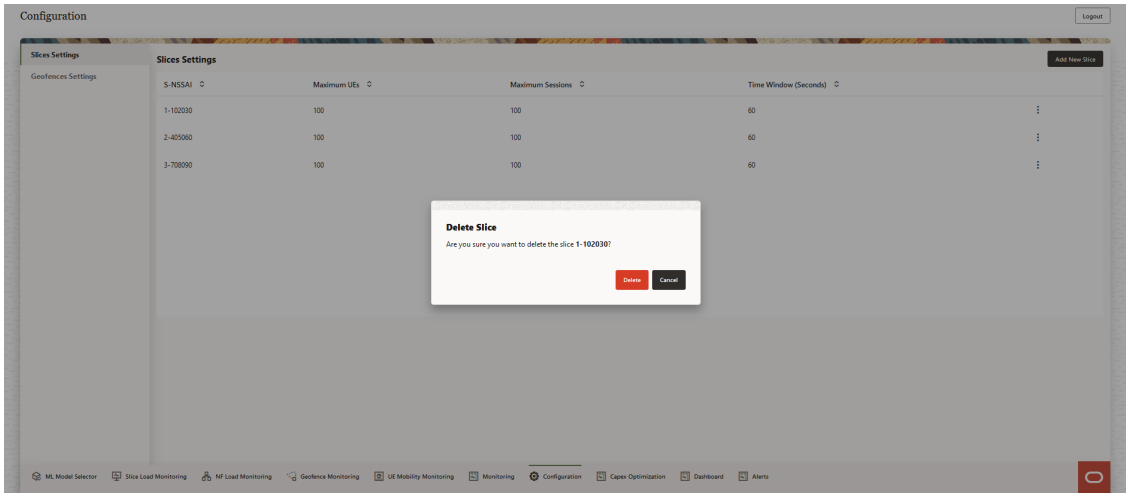
Modify the required fields to edit the slice. Click **Save** to apply the changes to the slice. Click **Cancel** to discard the changes.

8.8.1.3 Delete Slice

To delete a slice, click the vertical **Ellipses** icon on the right side of the slice to be deleted. Click **Delete** option that appears in a pop-up window.

A **Delete Slice** confirmation dialog box appears on the screen.

Figure 8-30 Delete Slice



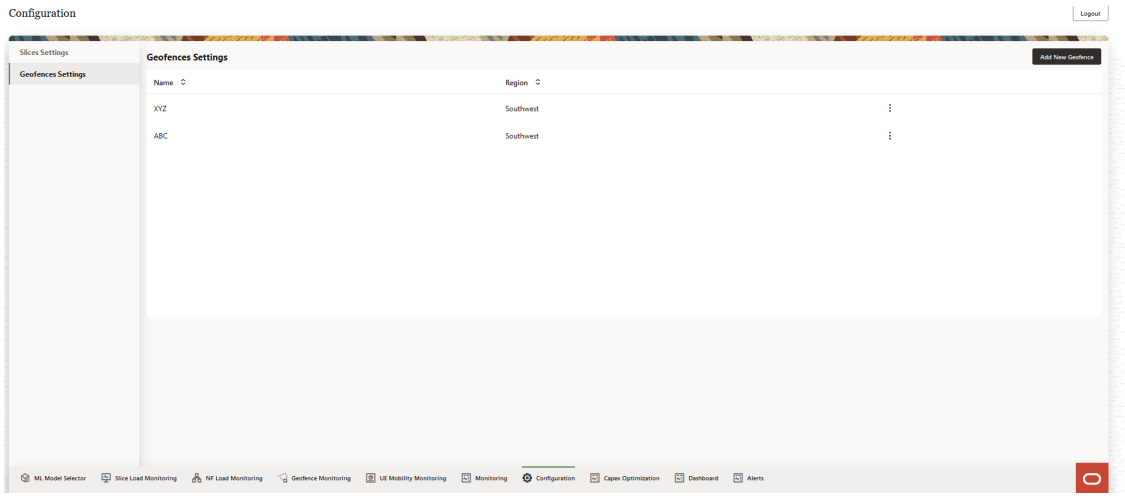
Click **Delete** to confirm deletion or **Cancel** to discard slice deletion.

After the slice is successfully deleted, a **Success** message appears on the screen.

8.8.2 Geofence Settings

The **Geofence Settings** page provides an option to **Add New Geofence** and view the **Geofence Settings** of all the configured geofences.

Figure 8-31 Geofences Settings



The user can perform the following actions on the **Geofences Settings** screen:

- Add New Geofence
- View the configured geofences and the geofence parameters:
  - **Name**

- **Region**

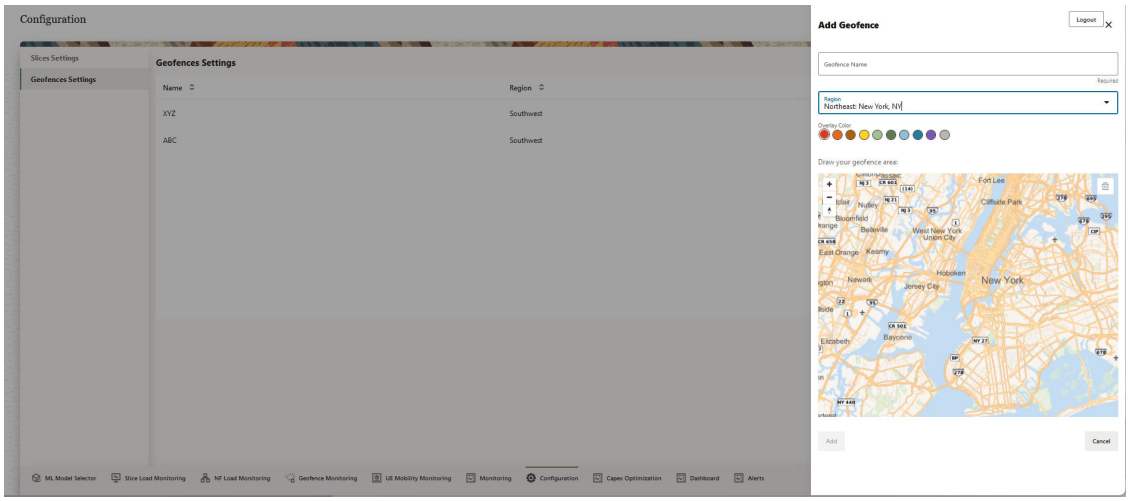
  Use the **Arrow** icon provided for each of the above parameters to list the values in ascending order.

- Click the vertical **Ellipses** icon to edit a geofence. The Edit Geofence option appears in a pop-up window.
- Click the vertical **Ellipses** icon to delete a geofence. The Delete Geofence option appears in a pop-up window.

8.8.2.1 Add New Geofence

To add a new geofence, click **Add New Geofence** in the **Geofence Settings** screen. A form with the fields to add a new geofence **Add Geofence**, appears on the right side of the screen:

Figure 8-32 Add Geofence



Provide the following information to create a new geofence:

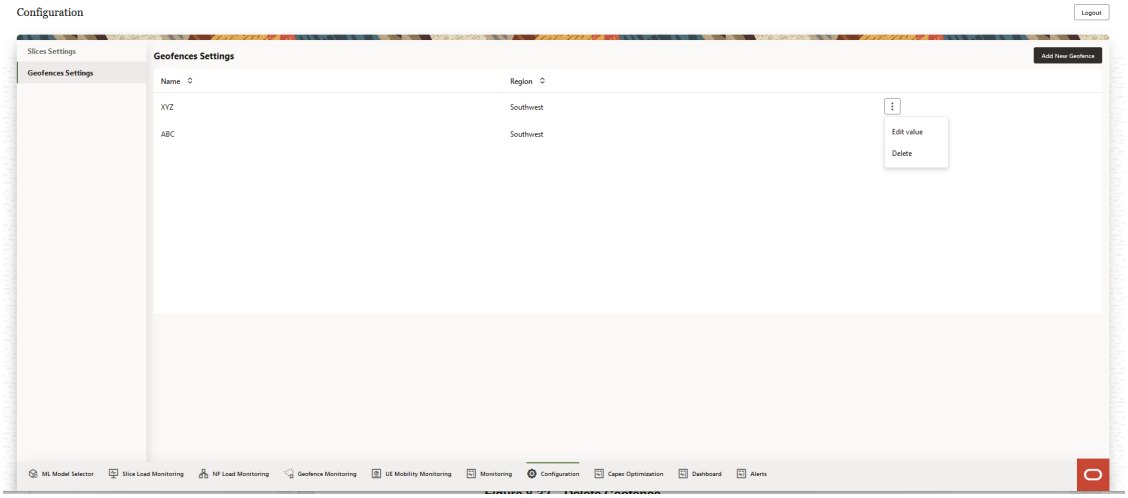
- Provide a **Geofence Name**. This is a required field.
- Select **Region** from the drop-down list.
- Select an **Overlay Color** for the geofence.
- A map to **Draw your geofence area** appears on the screen. Click on the map to select the geofence co-ordinates, the region formed by the co-ordinates defines the geofence area.

Click **Add** to create a new geofence. A success message appears on the screen. The new geofence is listed on the **Geofence Settings** screen. Click **Cancel** to discard the changes.

8.8.2.2 Edit Geofence

To edit a geofence, click the vertical **Ellipses** icon on the right side of the geofence to be edited.

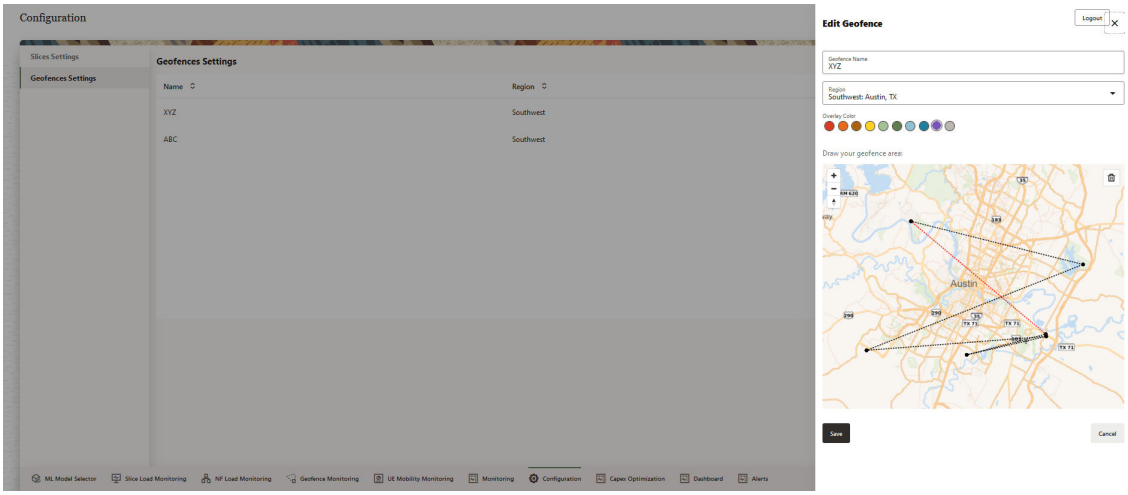
Figure 8-33 Edit Value



Click the **Edit Value** option that appears in a pop-up window.

The **Edit Geofence** form appears on the right side of the screen.

Figure 8-34 Edit Geofence



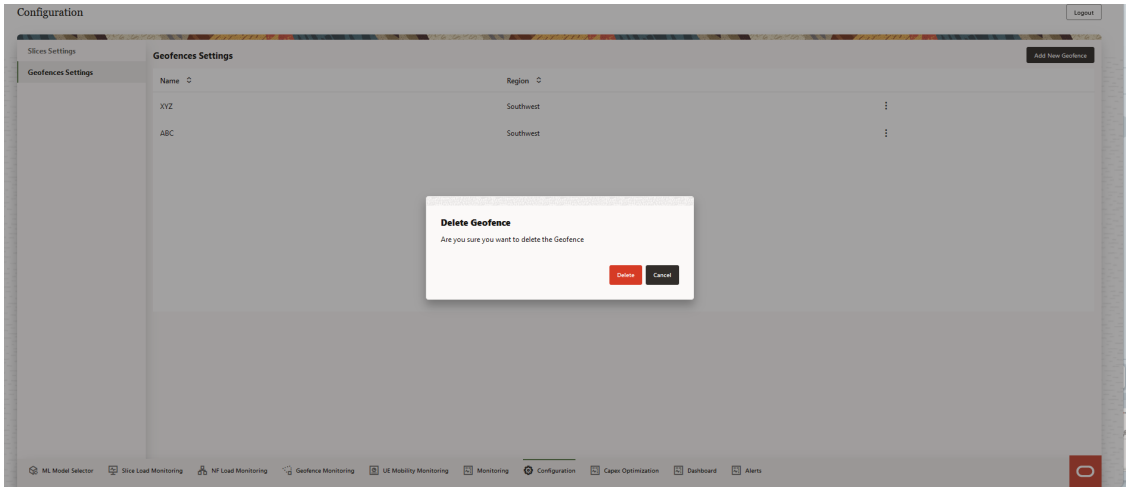
Modify the required fields to edit the geofence. Click **Save** to apply the changes to the geofence or click **Cancel** to discard the changes.

8.8.2.3 Delete Geofence

To delete a geofence, click the vertical **Ellipses** icon on the right side of the geofence to be deleted. Click **Delete** option that appears in a pop-up window.

A **Delete Geofence** confirmation dialog box appears on the screen.

Figure 8-35 Delete Geofence



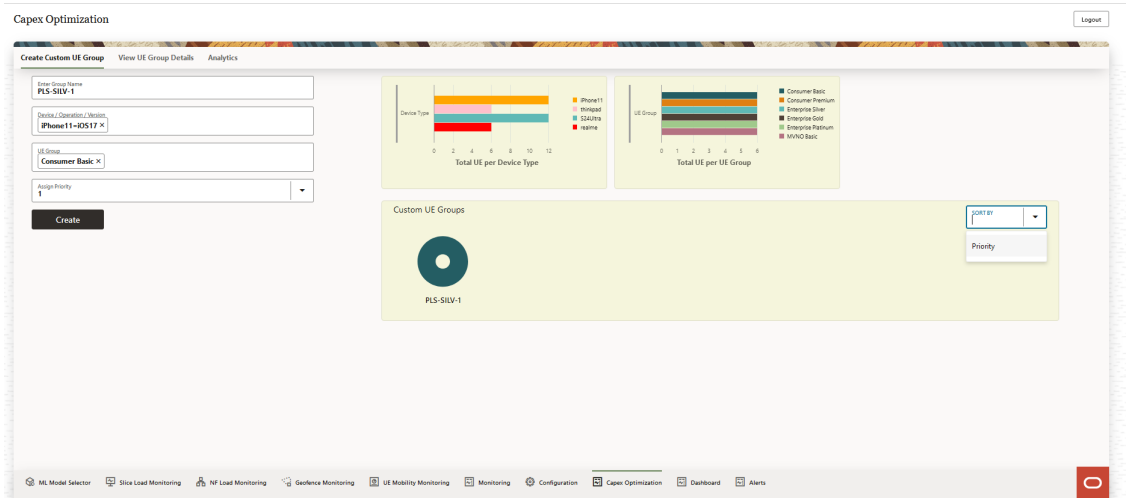
Click **Delete** to confirm deletion or **Cancel** to discard geofence deletion.

After the geofence is successfully deleted, a **Success** message appears on the screen.

8.9 Capex Optimization

The **Capex Optimization** screen displays tabs to **Create Custom UE Group**, **View UE Group Details** and view **Analytics** information.

Figure 8-36 Capex Optimization



Create Custom UE Group

Use the **Create Custom UE Group** tab to create UE groups. Enter the following information to create a UE group:

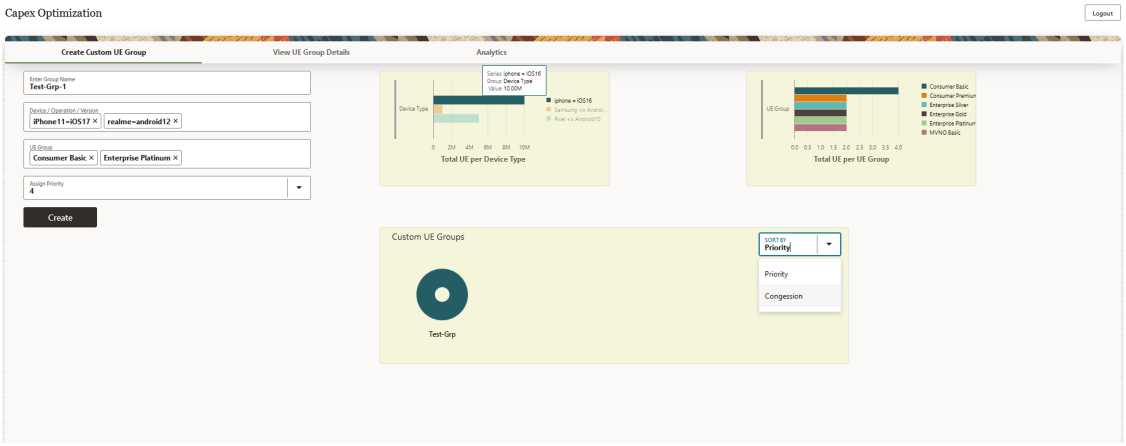
- **Enter Group Name**: Enter the desired group name.

- Select the **Device/Operation/Version**: Select the type of device. For example, **iphone11=iOS17**, **thinkpad=win11**, **realme=android12**, and so on.
- **UE Group**: Select the UE group, to which the custom UE group must belong. For example **Consumer Basic**, **Enterprise Platinum**, **MVNO Basic**, **Enterprise Gold**, **Enterprise Silver** and so on.

Assign Priority for the custom UE group. You can assign any value from "1" up to "5".

Click **Create** to create a new custom UE group. A success message appears on the screen.

Figure 8-37 Create UE Group



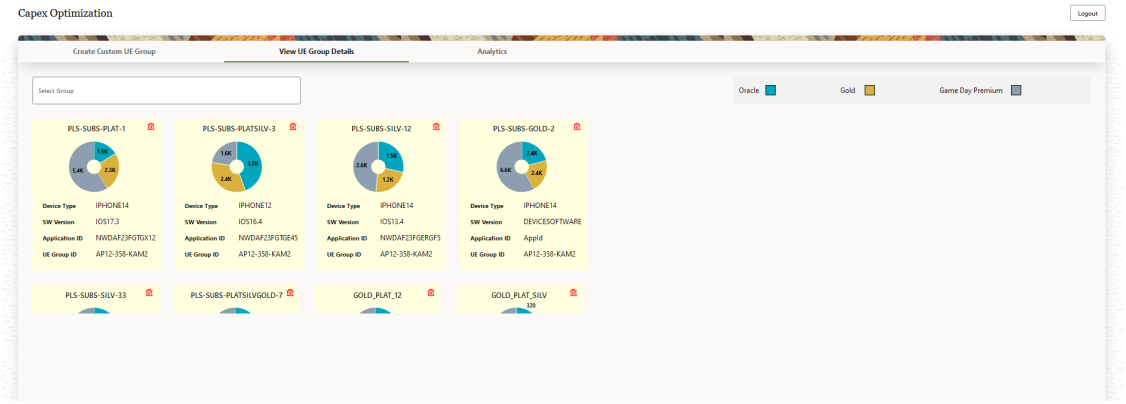
This tab also displays graphical representation of **Total UE per Device Type** and **Total UE per UE Group**. The different device types are color coded on the graph.

A graphical representation of the configured **Custom UE Groups** is displayed on the screen. You can sort the configured **Custom UE Groups** displayed on the screen by selecting either **Priority** or **Congestion** from the drop-down list. The UE groups are color coded. The **Custom UE Groups** are displayed as a composition of various color coded UE groups. Hover the mouse on the graph to view more details.

View UE Group Details

This tab displays composition graphs of all the configured **Custom UE Groups** along with **Device Type**, **SW Version**, **Application ID**, and **UE Group ID** information.

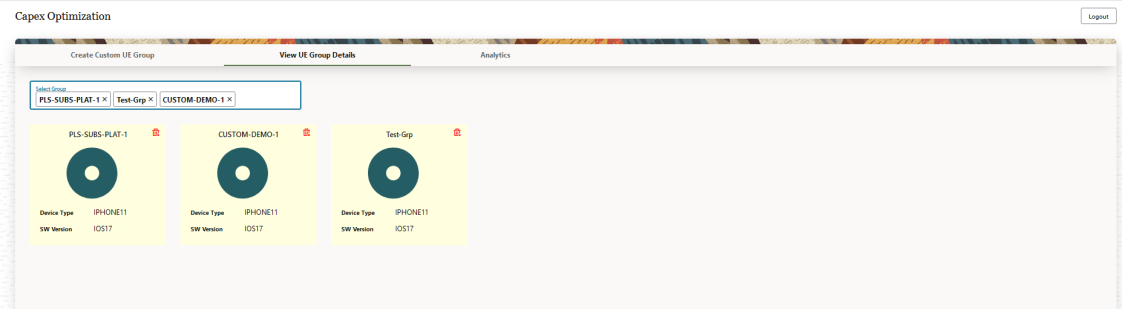
Figure 8-38 View UE Group Details



Use the **Select Group** option to select the groups for which you want to view the composition graphs.

For example:

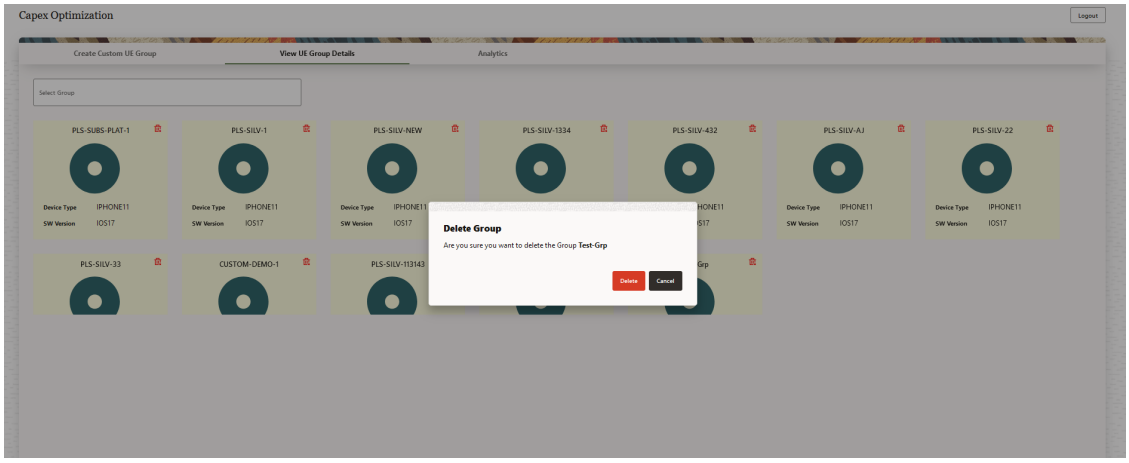
Figure 8-39 Select Group



To delete any UE group, click **Delete** icon displayed on that group's graph.

To confirm deletion, the following screen appears:

Figure 8-40 Delete Group



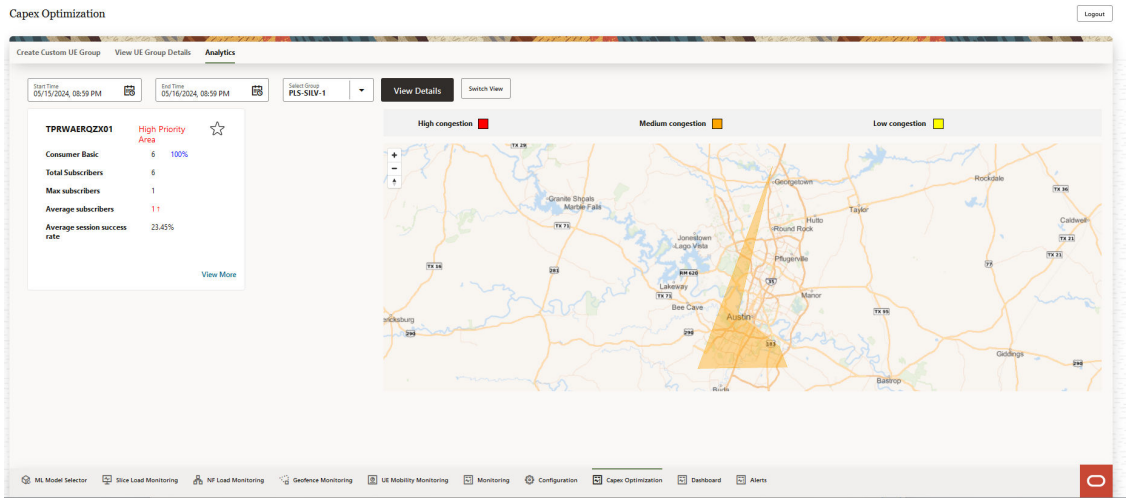
Click **Delete** to confirm the operation. Click **Cancel** to discard the operation.

Analytics

Use this tab to view **Analytics** information for the selected group. Select the **Start Time**, **End Time**, and **Select Group** (from the drop-down list) and click **View Details** to view analytics information.

For example:

Figure 8-41 View Details



Congestion levels are categorized as below:

- **High Congestion**
- **Medium Congestion**
- **Low Congestion**

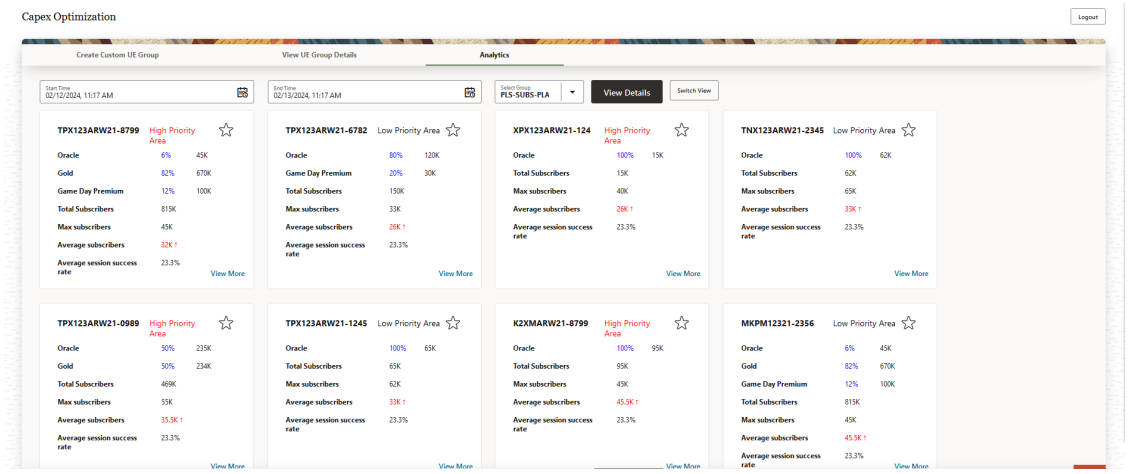
The congestion levels are color coded and displayed on the screen. The congestion levels in the tracking areas are displayed in the map view.

The tracking area is displayed in the map view. Use **+** and **-** icons to zoom in or out the map view.

Use the **Switch View** button to switch between tracking area analytics view and map view. In the map view, the tracking area information is displayed on the left side of the screen.

Sample tracking area analytics view:

Figure 8-42 Tracking Area View



The following information is displayed for each tracking area:

- The tracking area's ID. For example, **TPX123ARW21-8799**.
- The priority as either **High Priority Area** or **Low Priority Area**.
- You can mark the tracking area as "starred" by clicking on the **Star** icon.
- The **UE Groups**, the number of subscribers in that UE group, and the UE group's % composition of subscribers in that tracking area. For example **Oracle**, **50 %**, and **235K**.
- The **Total Subscribers** count.
- The **Max Subscribers** count.
- The **Average Subscribers** count.
- The **Average Session Success Rate**.
- Click **View More** option to see detailed information of the selected tracking area in a new window.

View More

This screen displays detailed information about the selected tracking area. Select the **Start Time** and **End Time** to see the tracking area analytics for specified time interval.

Click **Go Back** to return to previous screen.

Figure 8-43 View More

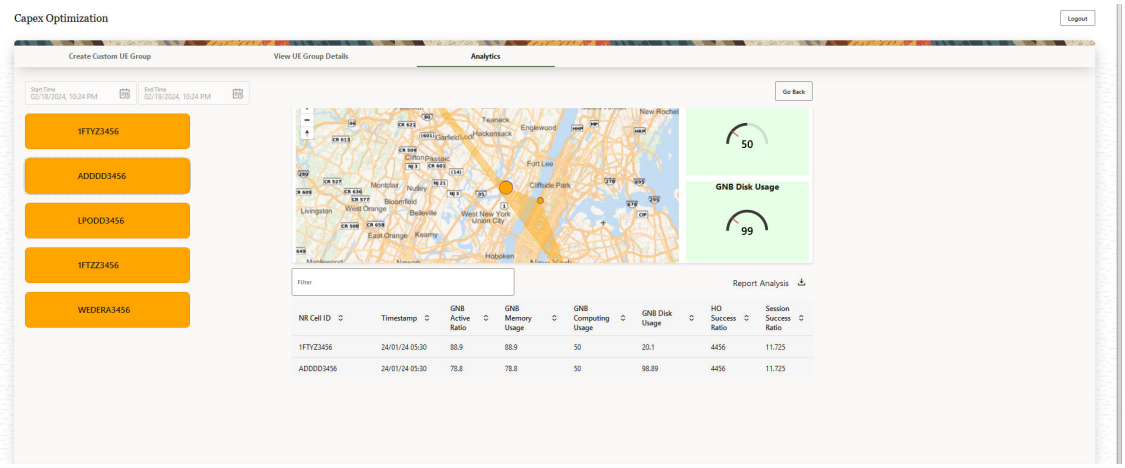
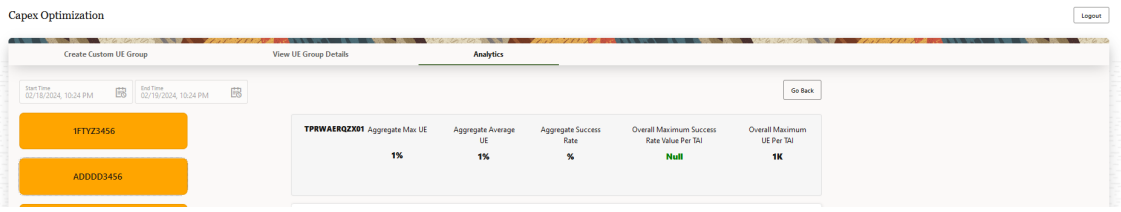


Figure 8-44 Tracking Area Information



The following information is displayed on the screen:

- The **Tracking Area Id**. For example, **TPX123ARW21-8799**.

- The **Aggregate Max UE** as a percentage value.
- The **Aggregate Average UE** as a percentage value.
- The **Aggregate Success Rate** as a percentage value.
- The **Overall Maximum Success Rate Value Per TAI** value.
- The **Overall Maximum UE Per TAI** value.

The tracking area is displayed in the map view. The cells in the tracking area are marked. Use **+** and **-** icons to zoom in or out the map view.

List of cells (with **Cell Id**) in the tracking area is displayed on the left side of the screen. Click **Cell Id**, the cell is highlighted in the map view and the following information is displayed adjacent to the map view:

- **GNB Computing Usage**
- **GNB Disk Usage**

Use the **Filter** text box to specify the filter information. Click **Download** icon to download the **Report Analysis**.

The following cell information is listed on the screen:

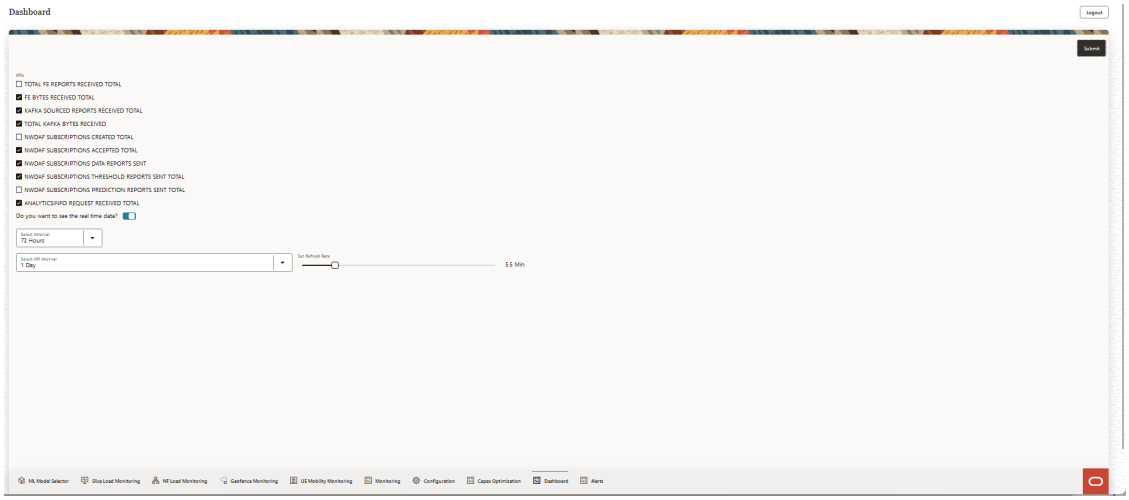
- **NR Cell ID**
- **Timestamp**
- **GNB Active Ratio**
- **GNB Memory Usage**
- **GNB Computing Usage**
- **GNB Disk Usage**
- **HO Success Ratio**
- **Session Success Ratio**

Use the **Arrow** icon provided for each of the above parameters to list the values in ascending order.

8.10 Dashboard

The **Dashboard** page displays OCNWDAF Key Performance Indicators (KPIs), offers the option to view real-time data, and allows users to filter the KPIs based on time interval, KPI interval, and refresh rate.

Figure 8-45 Dashboard



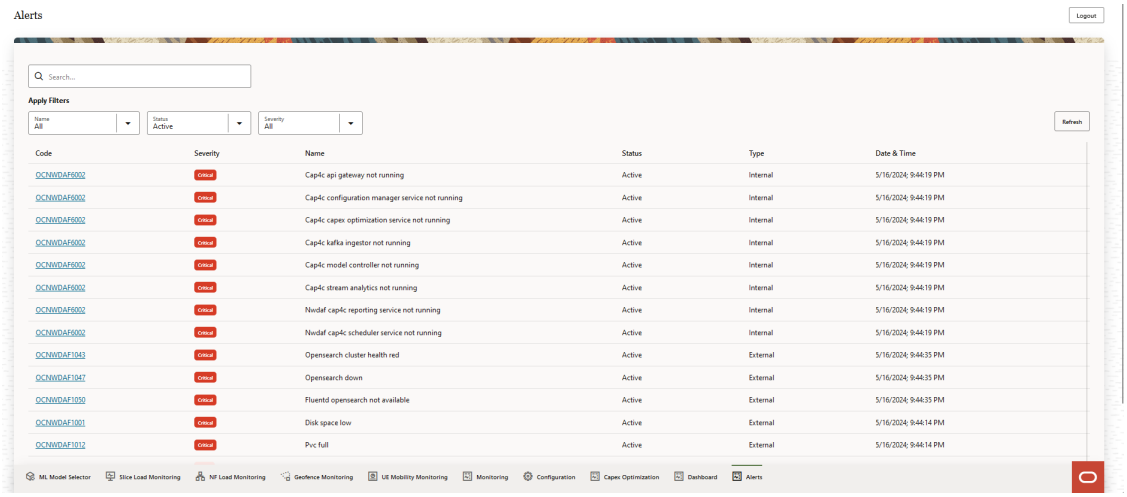
To view detailed information on the selected KPIs, follow the procedure below:

1. Select the check box provided for the KPIs listed on the screen.
2. Use the toggle switch **Do you want to see the real time data?** to view real-time data.
3. Provide the **Start Time** and **End Time** interval.
4. **Select KPI Interval** from the drop-down list. The available options are **5 Mins**, **15 Mins**, **30 Mins**, **1 Hour**, and **1 Day**.
5. Use the slider to **Set Refresh Rate**, select any value between **0.5** Mins up to **12.5** Mins.
6. Click **Submit**.
7. A new window with detailed information on the selected KPIs appears on the screen. To return to the previous screen, click **Metrics Settings**.

8.11 Alerts

The **Alerts** page displays the list of alerts generated by OCNWDAF.

Figure 8-46 Alerts



Use the **Search** bar to search for a particular alert.

Apply Filters and view the desired alerts. You can filter the alerts based on:

- **Name**: Select an option from the following options in the drop-down list.
- **Status**: Select an option from the following options in the drop-down list.
- **Severity**: Select an option from the following options in the drop-down list **All**, **Critical**, **Major**, **Minor**, **Info**, or **Warning**.

Click **Refresh** to refresh the table of alerts.

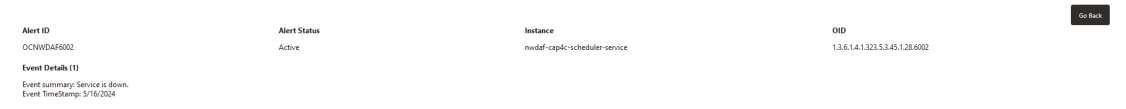
List of alerts with the following information is displayed:

- **Code**
- **Severity**
- **Name**
- **Status**
- **Type**
- **Date & Time**

Click alert **Code**, a new window with detailed information on the alert appears on the screen.

For example:

Figure 8-47 Alert Information



This screen displays the following alert information:

- **Alert ID**
- **Alert Status**
- **Instance**
- **OID**
- **Event Detail**

Click **Go Back** to return to the **Alerts** page.

9 Supported REST API Interfaces

This chapter describes the REST APIs supported by OCNWDAF.

9.1 Analytics Subscription Service

REST APIs create, modify, and delete OCNWDAF Event Subscriptions. REST APIs also send notifications about the observed event to the consumer NF.

Create an OCNWDAF Event Subscription

URI: `{apiRoot}/nwdaf-eventssubscription/v1/subscriptions`

Method: POST

Request Body:

Type: *NnwdafEventsSubscription*

Table 9-1 Request Body Parameters

Name	Data Type	P	Cardinality	Description
NnwdafEventsSubscription	Object	M	1	Creates a new individual OCNWDAF event subscription resource using a POST request.

Response:

Table 9-2 Supported Response Codes

Response Code	Description
201 Created	The response to successfully creating an OCNWDAF event subscription using a POST request. The stored subscribed event is returned.
400 Bad Request	The response to a POST request if the create subscription request does not contain valid data.
500 Internal Server Error	The response to a request if there is an internal server processing error.

Delete an OCNWDAF Event Subscription using SubscriptionID

URI: `{apiRoot}/ocnwdaf-eventssubscription/v1/subscriptions/{subscriptionId}`

Method: DELETE

Response:

Table 9-3 Supported Response Codes

Response Code	Description
204 No Content	The response to a successful delete subscription request.
404 Not found	The response to a DELETE request if the subscription is not found.
500 Internal Server Error	The response to a request if there is an internal server processing error.

Notify the Consumer NF about an observed event

URI: Notification URI

Method: POST

Request Body:

Type: *NnwdafEventsSubscriptionNotification*

Table 9-4 Request Body Parameters

Name	Data Type	P	Cardinality	Description
NnwdafEventsSubscriptionNotification	Array	M	1 up to N	Provides information about observed events.

Response:

Table 9-5 Supported Response Codes

Response Code	Description
204 No Content	The response to a successful notification event.
500 Internal Server Error	The response to a request if there is an internal server processing error.

9.2 Analytics Information Service

REST APIs are used to obtain analytics information from the Analytics Database service. The Analytics information service invokes Data collection and Analytics generation services by sending POST requests with specific AnalyticsIDs.

Retrieve OCNWDAF analytics information

URI: `{apiRoot}/nnwdaf-analyticsinfo/v1/analytics`

Method: GET

Request Body:

Type:

Table 9-6 Request Body Parameters

Name	Data Type	P	Cardinality	Description
ana-req	EventReportingRequirement	O	0 to 1	Specifies the analytics event reporting requirement information.
event-id	EventId	M	1	Included to identify the analytics.
event-filter	EventFilter	C	0 to 1	Included to identify the analytics when filter information is needed for the related event.
supported-features	SupportedFeatures	O	0 to 1	Filters irrelevant responses related to unsupported features.
tgt-ue	TargetUeInformation	O	0 to 1	Identifies the target UE information.

Response:

Table 9-7 Supported Response Codes

Response Code	Description
200 OK	A successful response, returned with requested analytics information in the message body.
204 No Content	Response if the requested analytics data does not exist.
400 Bad Request	Response to the request: • When NF consumers request both statistical and predictive analytics. • When the requested supportedFeatures or AnalyticsID is not valid. • When the request has invalid optional parameters. • In the absence of EventFilter in Request Parameters for data collection.
422 Unprocessable Entity	The response for the request when OCNWDAF-NRFClient is not registered.
500 Internal Server Error	The response to a request if there is an internal server processing error.

9.3 OCNWDAF Analytics APIs

The 5G NFs can subscribe (or cancel) to a specific network analytics and also obtain a network analytics report for a particular context from the OCNWDAF. The analytics supported are Slice Load Level, UE Mobility, UE Abnormal Behavior, NF Load Level, Network Performance Analytics, User Data Congestion Analytics, and QoS Sustainability Analytics.

> **Note**
>
> **Pre-requisites:**
>
> - The NRF is deployed and running.
> - The OCNWDAF is deployed and running.
> - The Notification microservice is deployed and running.
> - OCNWDAF profile is created.
> - OCNWDAF token is created.

APIs are invoked to obtain the following analytics information:

- UE Abnormal Behavior Analytics
- Slice Load Level Analytics
- UE Mobility Analytics
- NF Load Analytics
- Network Performance Analytics
- User Data Congestion Analytics
- QoS (Quality of Service) Sustainability Analytics

9.3.1 UE Abnormal Behavior Analytics

This service operation is used to subscribe to UE Abnormal Behavior Analytics.

Type: POST

URI: `{apiRoot}/nnwdaf-eventssubscription/v1/subscriptions/`

Initiated By: Consumers

Table 9-8 Request Body Parameters

Field Name	Data Type	Description
eventSubscriptions	EventSubscription	Specifies the subscribed event. The event parameter within the subscription is set to "ABNORMAL_BEHAVIOUR".
notificationURI	Uri	The URI which receives the requested notifications from the OCNWDAF. This parameter is provided by the NF service consumer in the HTTP POST request that creates the subscriptions for event notifications.
supportedFeatures	SupportedFeatures	This parameter is provided by the NF service consumer in the POST request for creating an OCNWDAF Event Subscription resource, and it is also provided in response to the corresponding request.

Table 9-8 (Cont.) Request Body Parameters

Field Name	Data Type	Description
evtReq	ReportingInformation	Represents the reporting requirements of the event subscription. If this parameter is not provided, the default values for ReportingInformation is used. The notification method "notifMethod" within ReportingInformation takes precedence over the notificationMethod within EventSubscription.
immRep	Boolean	Immediate reporting indication. If this value is set to "true" the OC-NWDAF includes the reports of the events subscribed (if available), in the HTTP POST response.
notifMethod	String	Event notification method. The allowed values are: • ONE_TIME
maxReportNbr	Integer	Maximum number of reports.
monDur	Date time	Monitoring the duration.
eventSubscriptions	Array(EventSubscription)	A description of the subscribed events. It contains the following attributes: • event • tgtUe • exptAnaType • exptUeBehav
event	String	Indicates that the event subscribed is "ABNORMAL_BEHAVIOUR".
tgtUe	TargetUeInformation	Identifies the target UE information for which the subscription applies by "supis" and "anyUe" attributes.
exptAnaType	ExpectedAnalyticsType	Represents expected UE analytics type. It should be set to "COMMUN" Absent if the "excepRequs" attribute is provided.
exptUeBehav	ExpectedUeBehaviourData	Represents expected UE behaviour, it is used to define a geofence.
supis	Array	Identifies a SUPI for an UE.
anyUe	Boolean	Identifies any UE when set to true.
excepRequs	Array	Represents a list of Exception Ids with associated thresholds.
extraReportReq	EventReportingRequirement	The extra event reporting requirement information.
startTs	DateTime	UTC time indicating the start time of the observation period. The absence of this attribute means subscription at the present time.
endTs	DateTime	UTC time indicating the end time of the observation period. The absence of this attribute means subscription at the present time. If provided, it shall not be less than the start time.
notificationMethod	NotificationMethod	Indicates the notification method.

When the event parameter is "ABNORMAL_BEHAVIOUR", the following analytics are provided:

1. Identification of target UE(s) to which the subscription applies by "supis" or "anyUe" attribute in the "tgtUe" attribute.
2. Expected analytics type through the "exptAnaType" attribute.
3. Expected UE behavior through "exptUeBehav" attribute.
4. Either "excepRequs" or "exptAnaType" shall be provided if subscribed event is "ABNORMAL_BEHAVIOUR".

> **Note**
>
> The data types supported by OCNWDAF comply with the 3GPP specifications. For more information about the 3GPP data types, see 3GPP Technical Specification 29.520, Release 16, Network Data Analytics Services.

Table 9-9 Supported Response Codes

Code	Description
201	The subscription resource is created successfully.
400	Bad Request. The request is incorrect and subscription is not created.
500	Indicates a internal server processing error.

Examples

The following example shows how an NF creates a subscription request for UE Abnormal Behavior Analytics by submitting a POST request on the REST resource using cURL.

cURL Command

```
curl --location --request POST '{HTTP_ENDPOINT}' \--header 'Content-Type:
application/json' \--data-raw '{JSON_OBJECT}'
```

Example of the Request Body

```
{
  "eventSubscriptions": [
    {
      "anySlice": false,
      "event": "ABNORMAL_BEHAVIOUR",
      "extraReportReq": {
        "startTs": "2024-08-25T17:18:40.694Z",
        "endTs": "2024-08-30T18:58:40.694Z",
        "offsetPeriod": 0,
        "sampRatio": 75,
        "maxObjectNbr": 0,
        "maxSupiNbr": 0,
      },
      "notificationMethod": ON_EVENT_DETECTION,
      "networkArea": null,
      "tgtUe": {
        "anyUe": false,
        "supis": [
```

```
            "imsi-334410291417776"
          ],
          "gpsis": null,
          "intGroupIds": null
        },
        "exptAnaType": "COMMUN" [Mandatory],
        "exptUeBehav": {
          "communicationDurationTime": 0, [Mandatory]
          "periodicTime": 0, [Mandatory]
          "scheduledCommunicationTime": {
            "daysOfWeek": [
              7
            ],
            "timeOfDayStart": "2023-03-28T19:10:30.000000",
            "timeOfDayEnd": "2023-03-29T19:10:30.000000"
          } [Mandatory],
          "scheduledCommunicationType": "BIDIRECTIONAL" [Mandatory],
          "trafficProfile": "SINGLE_TRANS_UL" [Mandatory]
        }
      }
    ],
    "evtReq": {
      "immRep": false,
      "notifMethod": "ONE_TIME",
      "maxReportNbr": 100,
      "monDur": "2023-11-01T14:00:05Z",
      "repPeriod": 0,
      "sampRatio": 75,
      "partitionCriteria": null,
      "grpRepTime": 0,
      "notifFlag": null
    },
    "notificationURI": "http://10.75.245.241:30098/notification",
    "supportedFeatures": "010",
    "eventNotifications": null,
    "failEventReports": null,
    "prevSub": null,
    "consNfInfo": null
}
```

9.3.2 Slice Load Level Analytics

This service operation is used to subscribe to Slice Load Level Analytics.

Type: POST

URI: `{apiRoot}/nnwdaf-eventssubscription/v1/subscriptions/`

Initiated By: Consumers

Table 9-10 Request Body Parameters

Field Name	Data Type	Description
notificationURI	uri	The URI which receives the requested notifications from the OCNWDAF. This parameter provided by the NF service consumer in the HTTP POST request that creates the subscriptions for event notifications.
supportedFeatures	SupportedFeatures	The supported feature number.
evtReq	ReportingInformation	Is the event reporting information applicable for each event. It contains the following attributes: • immRep • notifMethod • maxReportNbr • monDur
immRep	boolean	Immediate reporting indication. This value is set to "true" the OC-NWDAF includes the reports of the events subscribed, if available, in the HTTP POST response.
notifMethod	string	Event notification method. The allowed values are: • ON_EVENT_DETECTION • ONE_TIME • PERIODIC
maxReportNbr	integer	Maximum Number of Reports.
monDur	Date time	Monitoring duration.
eventSubscriptions	array(EventSubscription)	A description of the subscribed events. It contains the following attributes: • event • anySlice • loadLevelThreshold • notificationMethod • snssaia
event	string	Indicates that the event subscribed is load level information of Network Slice, "SLICE_LOAD_LEVEL"
anySlice	boolean	• True: Indicates applicable to all slices. • False: Indicates not applicable to all slices.
loadLevelThreshold	integer	The OCNWDAF reports the corresponding network slice load level to the NF service consumer when the load level of the network slice identified by snssais has reached.
notificationMethod	NotificationMethod	Indicates the notification method. The allowed values are: • PERIODIC: The subscription of OCNWDAF event is periodic. • THRESHOLD: The subscription of OCNWDAF event is on exceeding threshold value.
matchingDir	MatchingDirection	This is an optional parameter. A matching direction can be provided along with a threshold. The options are "DESCENDING", "ASCENDING", and "CROSSED". The default value is "CROSSED".

Table 9-10 (Cont.) Request Body Parameters

Field Name	Data Type	Description
snssaia	String	Identifies of network slice to which the subscription belongs.
sst	Uinteger	Unsigned integer, within the range 0 up to 255, representing the Slice or Service Type.
sd	String	3-octet string, representing the Slice Differentiator, in hexadecimal representation.

When the event parameter is "SLICE_LOAD_LEVEL", the following analytics are provided:

1. The Network slice load level threshold in the "loadLevelThreshold" attribute if the "notifMethod" attribute in "evtReq" attribute is "ON_EVENT_DETECTION" or the "notificationMethod" attribute in "eventSubscriptions" attribute is "THRESHOLD" or "OMITTED".
2. Identification of network slice(s) to which the subscription applies through the identification of network slice(s) in the "snssais" attribute or as indicated in the "anySlice" attribute.

> **Note**
>
> The data types supported by OCNWDAF comply with the 3GPP specifications. For more information about the 3GPP data types, see 3GPP Technical Specification 29.520, Release 16, Network Data Analytics Services.

Table 9-11 Supported Response Codes

Code	Description
201	The subscription resource is created successfully.
400	Bad Request. The request is incorrect and subscription is not created.
500	Indicates a internal server processing error.

Examples

The following example shows how an NF creates a subscription request for Slice Load Level analytics by submitting a POST request on the REST resource using cURL.

cURL Command

```
curl --location --request POST '{HTTP_ENDPOINT}' \--header 'Content-Type:
application/json' \--data-raw '{JSON_OBJECT}'
```

Example of the Request Body

```
{ "notificationURI": "https://{CONSUMERAPIROOT}/notification",
"supportedFeatures": "100",
"evtReq": {
        "immRep": false,
        "notifMethod": "ON_EVENT_DETECTION",
```

```
        "maxReportNbr": 0,
        "monDur": "2022-06-24T04:00:00Z" }
"eventSubscriptions": [{
"event": "SLICE_LOAD_LEVEL",
"anySlice": false,  "loadLevelThreshold": 10,
"notificationMethod": "THRESHOLD",
"matchingDir": "ASCENDING",
"snssaia": [
                {
                    "sd": "708090"
                    "sst": "3",

                }
            ]
 }]}
```

9.3.3 UE Mobility Analytics

This service operation is used to subscribe to UE Mobility Analytics.

Type: POST

URI: `{apiRoot}/nnwdaf-eventssubscription/v1/subscriptions/`

Initiated By: Consumers

Table 9-12 Request Body Parameters

Field Name	Data Type	Description
notificationURI	uri	The URI which receives the requested notifications from the OCNWDAF. This parameter provided by the NF service consumer in the HTTP POST request that creates the subscriptions for event notifications.
supportedFeatures	SupportedFeatures	The supported feature number.
evtReq	ReportingInformation	Is the event reporting information applicable for each event. It contains the following attributes: • immRep • notifMethod • maxReportNbr • monDur
immRep	boolean	Immediate reporting indication. This value is set to "true" the OC-NWDAF includes the reports of the events subscribed, if available, in the HTTP POST response.
notifMethod	string	Event notification method. The allowed value is: • ONE_TIME
maxReportNbr	integer	Maximum Number of Reports.
monDur	Date time	Monitoring duration.
eventSubscriptions	array(EventSubscription)	A description of the subscribed events. It contains the following attributes: • event • tgtUe • networkArea

Table 9-12 (Cont.) Request Body Parameters

Field Name	Data Type	Description
event	string	Indicates that the event subscribed is "UE_MOBILITY".
tgtUe	TargetUeInformation	Identifies the target UE information for which the subscription applies by "supis" , "intGroupIds" and "anyUe" attributes.
networkArea	NetworkAreaInfo	Identification of network area to which the subscription applies.
supis	array	Identifies a SUPI for an UE.
intGroupIds	array	Represents an internal group identifier and identifies a group of UEs.
anyUe	boolean	Identifies any UE when set to true.

When the event parameter is "UE_MOBILITY", the following analytics are provided:

1. Identification of target UE(s) to which the subscription applies by "supis" or "intGroupIds" attribute in the "tgtUe" attribute.
2. Identification of network area to which the subscription applies through the identification of network area by "networkArea" attribute.

> **Note**
>
> The data types supported by OCNWDAF comply with the 3GPP specifications. For more information about the 3GPP data types, see 3GPP Technical Specification 29.520, Release 16, Network Data Analytics Services.

Table 9-13 Supported Response Codes

Code	Description
201	The subscription resource is created successfully.
400	Bad Request. The request is incorrect and subscription is not created.
500	Indicates a internal server processing error.

Examples

The following example shows how an NF creates a subscription request for UE Mobility Analytics by submitting a POST request on the REST resource using cURL.

cURL Command

```
curl --location --request POST '{HTTP_ENDPOINT}' \--header 'Content-Type:
application/json' \--data-raw '{JSON_OBJECT}'
```

Example of the Request Body

```
{ "notificationURI": "https://{CONSUMERAPIROOT}/notification",
"supportedFeatures": "002",
```

```
"evtReq": {
        "immRep": "false",
        "notifMethod": "ONE_TIME",
        "maxReportNbr": 0,
        "monDur": "2022-06-24T04:00:00Z" },
"eventSubscriptions": [{
"event": "UE_MOBILITY",
"tgtUe": {
    "supis": ["{VALIDSUPID}"],
    "intGroupIds": null,
    "anyUe": false  },
    "networkArea": null
    }]
}
```

9.3.4 NF Load Analytics

This service operation is used to subscribe to NF Load Analytics.

Type: POST

URI: `{apiRoot}/nnwdaf-eventssubscription/v1/subscriptions/`

Initiated By: Consumers

Table 9-14 Request Body Parameters

Field Name	Data Type	Description
AnySlice	boolean	Default is FALSE. If TRUE ignore any snssais, array of Snssai or slice IDs.
event	string	Event that is subscribed, in this case "NF_LOAD".
networkArea	array	Identification of network area to which the subscription applies. The absence of networkArea means subscription to all network areas. **Note:** It should be set to "null". It is an optional field.
startTs	date format in UTC timezone	UTC time indicating the start time of the observation period. The absence of this attribute means subscription at the present time.
endTs	date format in UTC timezone	UTC time indicating the end time of the observation period. The absence of this attribute means subscription at the present time. If provided, it should not be less than the start time.
notificationMethod	string	Indicates the notification method. When notificationMethod is not provided, the default value is "THRESHOLD".
matchingDir	boolean	A matching direction may be provided alongside a threshold. If omitted, the default value is CROSSED. This field is optional.

Table 9-14 (Cont.) Request Body Parameters

Field Name	Data Type	Description
nfLoadLvlThds		Indicates when the reporting should start after the after the average load level is reached. This field is provided if the "notifMethod" in "evtReq" is set to "ON_EVENT_DETECTION" or "notificationMethod" in "eventSubscriptions" is set to "THRESHOLD" or omitted. • "congLevel": integer • "nfLoadLevel": integer, • "nfCpuUsage": integer, • "nfMemoryUsage": integer, • "nfStorageUsage": integer
nfInstanceIds	array	An array of Identification(s) of NF instances. This field is optional.
nfSetIds	array	An array of Identification(s) of NF instance sets. This field is optional.
nfTypes	array	An array of Identification(s) of NF types. This field is optional.
snssais	array	Identification(s) of network slice to which the subscription applies. This field is optional and should be set to NULL.
tgtUe	array(TargetUeInformation) • anyUe, boolean • supis, array of Supi	Only applicable to determine AMF or SMF (from the SUPI). Identifies target UE information.
exptAnaType	string	It should be set to "MOBILITY" Represents expected UE analytics type. Absent if the "excepRequs" attribute is provided.
evtReq	array	Should be ON_EVENT_DETECTION if thresholds are defined, or notificationMethod is THRESHOLD. Represents the reporting requirements of the event subscription. If omitted, the default values within the ReportingInformation data type apply. • "immRep": false, **Set by default** • "notifMethod": "ON_EVENT_DETECTION", • "maxReportNbr": integer, • "monDur": date format in UTC timezone, • "repPeriod": integer and optional, • "sampRatio": integer and optional, • "grpRepTime": integer and optional
notificationURI	Uri	URI where to receive the requested notifications. Identifies the recipient of Notifications sent by the OCNWDAF.
supportedFeatures	string	This property should be “NfLoad”.

Table 9-15 Supported Response Codes

Code	Description
201	The subscription resource is created successfully.
400	Bad Request. The request is incorrect and subscription is not created.
500	Indicates a internal server processing error.

Examples

The following example shows how an NF creates a subscription request for NF load analytics by submitting a POST request on the REST resource using cURL.

cURL Command

```
curl --location --request PUT '{apiRoot}/nnwdaf-eventssubscription/v1/
subscriptions/' \--header 'Content-Type: application/json' \--data-raw
'{request_body}
```

Example of the Request Body

```
{
    "eventSubscriptions": [
        {
            "anySlice": true,
            "event": "NF_LOAD",
            "networkArea": null,
        "extraReportReq": {
            "startTs": "2022-09-06T05:00:30Z",
            "endTs": "2022-10-19T23:59:59Z"
        },
        "notificationMethod": "THRESHOLD",
        "matchingDir": null,
        "nfLoadLvlThds": [
            {
                "congLevel": 20,
                "nfLoadLevel": 20,
                "nfCpuUsage": 90,
                "nfMemoryUsage": 95,
                "nfStorageUsage": 80
            }
        ],
        "nfInstanceIds": null,
        "nfSetIds": null,
        "nfTypes": [
            "AMF",
            "SMF"
        ],
        "snssaia": null,
        "tgtUe": {
            "supis": null,
            "intGroupIds": null,
            "anyUe": false
```

```
        },
        "exptAnaType": "MOBILITY"
    }
],
"evtReq": {
    "immRep": false,
    "notifMethod": "ON_EVENT_DETECTION",
    "maxReportNbr": 50,
    "monDur": "2022-10-19T23:59:59Z",
    "repPeriod": 10,
    "sampRatio": 75,
    "grpRepTime": 0
},
"notificationURI": "{apiRoot}/notification",
"supportedFeatures": "040"
}
```

Example of the Response Body

```
{
    "eventSubscriptions": [
        {
            "anySlice": true,
            "event": "NF_LOAD",
        "extraReportReq": {
            "startTs": "2022-09-06T05:00:30Z",
            "endTs": "2022-10-19T23:59:59Z"
        },
        "notificationMethod": "THRESHOLD",
        "nfLoadLvlThds": [
            {
                "congLevel": 20,
                "nfLoadLevel": 20,
            }
        ],
        "nfTypes": [
            "AMF",
            "SMF"
        ],
        "congThresholds": [
            {
                "congLevel": 20,
                "nfLoadLevel": 50,
                "nfCpuUsage": 90,
                "nfMemoryUsage": 95,
                "nfStorageUsage": 80
            }
        ],
        "exptAnaType": "MOBILITY"
    }
],
"evtReq": {
    "immRep": false,
    "notifMethod": "ON_EVENT_DETECTION",
    "maxReportNbr": 50,
```

```
    "monDur": "2022-10-19T23:59:59Z",
    "repPeriod": 10,
    "sampRatio": 75,
    "grpRepTime": 0
},
"notificationURI": "{apiRoot}/notification",
"supportedFeatures": "040"
}
```

9.3.5 Network Performance Analytics APIs

Create a Network Performance Analytics Subscription

This service operation is used to create a Network Performance Analytics subscription.

Type: POST

URI: `{apiroot}:{serverPort}:/nnwdaf-eventsubscription/<api version>/subscriptions`

Table 9-16 Endpoint Parameters

Parameter	Description	Example
`{apiroot}`	The IP used to access the OCNWDAF subscription.	
`{serverport}`	The port used to access the OCNWDAF subscription. Default value is 8080.	
`{subscriptionId}`	Subscription ID	
`{analyticsId}`	The analytics ID is "NETWORK_PERFORMANCE"	
`{supported-features}`	080	
`{tgt-ue}`	Encoded Target UE information.	`{ "supis": null, "intGroupIds": null, "anyUe": true }`

Table 9-16 (Cont.) Endpoint Parameters

Parameter	Description	Example
{event-filter}	Encoded event filter value.	{ "anySlice": false, "networkArea": { "ncgis": [{ "plmnId": { "mcc": "375", "mnc": "36" }, "nrCellId": "eFdEDcE7D", "nid": "e5D8B1EbD11" }], "tais": [{ "plmnId": { "mcc": "585", "mnc": "162" }, "tac": "ebef4B",

Table 9-16 (Cont.) Endpoint Parameters

Parameter	Description	Example
		"nid": "fDfC6bbC673" }] }, "nwPerfTypes": ["NUM_OF_UE"] }
{ana-req}	Encoded value of analytics requirements.	{ "startTs":"2023-02-08T12:00:10.000021", "endTs":"2023-05-13T12:02:05.000000", "timeAnaNeeded":"2024-12-13T12:00:01.000000", "maxObjectNbr":10, "sampRatio":1 }

Initiated By: Consumers

Request Body Parameters

Table 9-17 Type NnwdafEventsSubscription

Parameter	Data Type	Presence	Description
eventSubscriptions	array(EventSubscription)	M	Subscribed events. The event parameter within event subscriptions is "NETWORK PERFORMANCE"

Table 9-17 (Cont.) Type NnwdafEventsSubscription

Parameter	Data Type	Presence	Description
evtReq	ReportingInformation	O	Represents the reporting requirements of the event subscription. If this parameter is not given then the default values for ReportingInformation is used. The notification method "notifMethod" within ReportingInformation takes precedence over notificationMethod within EventSubscription.
notificationURI	URI	C	URI to which the NWDAF sends the reports.
eventNotifications	array(EventNotification)	C	Notifications about Individual Events. Present only if the immediate reporting indication in the "immRep" attribute within the "evtReq" attribute is set to true in the event subscription, and the reports are available. Present in the response to NWDAF subscription if "immRep" is true and the reports are the available.
failEventReports	array(FailureEventInfo)	O	Supplied by the NWDAF. When this parameter is available,it contains the event(s) for which the subscription is not successful including the failure reason(s). This parameter is populated and returned in response to the error case.
consNfInfo	ConsumerNfInformation	O	Represents the analytics consumer NF information.
notifCorrId	String	M	Notification correlation ID. It is generated after successful subscription and is returned back in the response.
supportedFeatures	SupportedFeatures	C	This parameter is supplied by NF service consumer in the POST request for creation of an NWDAF Event Subscriptions resource, and supplied by the NWDAF in the reply of corresponding request. Value is "080" for Network Performance ID.

Table 9-18 Type EventSubscription

Parameter	Data Type	Presence	Description
event	NwdafEvent	M	Event that is subscribed. The value for network performance ID is "NETWORK PERFORMANCE"

Table 9-18 (Cont.) Type EventSubscription

Parameter	Data Type	Presence	Description
extraReportReq	EventReportingRequirement	O	The extra event reporting requirement information.
loadLevelThreshold	Integer	C	Indicates that the NWDAF shall report the corresponding network slice load level to the NF service consumer where the load level of the network slice identified by snssais is reached.
matchingDir	MatchingDirection	O	A matching direction may be provided alongside a threshold. If omitted, the default value is CROSSED.
networkArea	NetworkAreaInfo	C	Identification of network area to which the subscription applies. The absence of this parameter means the subscription is applicable to all the network areas.
notificationMethod	NotificationMethod	O	Indicates the notification method.
repetitionPeriod	DurationSec	C	Shall be supplied for notification method "PERIODIC" by the "notificationMethod" attribute.
tgtUe	TargetUeInformation	O	Identifies target UE information.
nwPerfRequs	array(NetworkPerfRequirement)		Represents the network performance requirements. This attribute shall be included when subscribed event is "NETWORK_PERFORMANCE". It may only be present if "appIds" attribute is provided.

Table 9-19 Type NnwdafEventsSubscriptionNotification

Parameter	Data Type	Presence	Description
eventNotifications	array (EventNotification)	C	Notifications about individual events.

Table 9-19 (Cont.) Type NnwdafEventsSubscriptionNotification

Parameter	Data Type	Presence	Description
subscriptionId	String	M	String identifying a subscription to the Nnwdaf_EventsSubscription service.

Table 9-20 Type EventNotification

Parameter	Data Type	Presence	Description
event	NwdafEvent	M	Subscribed events. The event parameter within event Subscriptions has to be "NETWORK PERFORMANCE"
start	DateTime	O	It defines the start time from when the analytics information becomes valid.
expiry	DateTime	O	It defines the expiration time after which the analytics information will become invalid.
timeStampGen	DateTime	C	It defines the timestamp of analytics generation.
duration	Duration	C	It defines the time period for which the threshold was in the target state.
nwPerfs	array(NetworkPerfInfo)	C	The network performance information.

Table 9-21 Supported Response Codes

Code	Description
201	The subscription is created successfully.
400	Bad Request. The request is incorrect and subscription is not created.
500	Indicates a internal server processing error.

Examples

The following example shows how an NF creates a subscription for Network Performance analytics by submitting a POST request on the REST resource using cURL.

cURL Command

```
curl --location '10.123.159.23:8087/nnwdaf-eventssubscription/v1/
subscriptions' \
--header 'accept: application/json' \
--header 'Content-Type: application/json' \
```

```
--data '{
    "notificationURI": "http://prodcon-1:9282/receive",
    "supportedFeatures": "080",
    "eventSubscriptions": [
        {
            "event": "NETWORK_PERFORMANCE",
            "extraReportReq": {
                "startTs": "2023-03-15T18:00:00Z",
                "endTs": "2023-03-16T18:30:00Z",
                "accuracy": null,
                "sampRatio": 70,
                "maxObjectNbr": 5,
                "maxSupiNbr": 2,
                "timeAnaNeeded": null
            },
            "loadLevelThreshold": 1,
            "nfLoadLvlThds": [
                {
                    "congLevel": 20,
                    "nfCpuUsage": 90,
                    "nfLoadLevel": 11,
                    "nfMemoryUsage": 95,
                    "nfStorageUsage": 80
                }
            ],
            "notificationMethod": "THRESHOLD",
            "snssaia": [
                {
                    "sst": 1,
                    "sd": "102030"
                }
            ],
            "tgtUe": {
                "supis": null,
                "intGroupIds": null,
                "anyUe": true
            },
            "nfInstanceIds": null,
            "nfSetIds": null,
            "matchingDir": "CROSSED",
            "networkArea": {
                "ncgis": [
                    {
                        "plmnId": {
                            "mcc": "375",
                            "mnc": "36"
                        },
                        "nrCellId": "0E0FB2773",
                        "nid": "e5D8B1EbD11"
                    }
                ],
                "tais": [
                    {
                        "plmnId": {
                            "mcc": "585",
                            "mnc": "162"
```

```
                        },
                        "tac": "ebef4B",
                        "nid": "fDfC6bbC673"
                    }
                ]
            },
            "nfTypes": [
                "AMF"
            ]
        }
    ],
    "evtReq": {
        "notifMethod": "ONE_TIME",
        "monDur": "2023-04-14T11:10:00Z",
        "immRep": false,
        "maxReportNbr": 2,
        "repPeriod": 1,
        "sampRatio": 70,
        "grpRepTime": 60
    }
}'
```

Example of the Request Body

```
{
    "eventSubscriptions": [
        {
            "anySlice": "N/A",
            "appIds": null,
            "dnns": null,
            "dnais": null,
            "event": "NETWORK_PERFORMANCE",
            //  necessary for subscribing to AMF  for number of UEs
            "networkArea": //   ---applicable if anyUE:true---
            //   29.554  - 5.6.2.8
            {
                "ncgis": [
                    {
                        "plmnId": {
                            "mcc": "375",
                            "mnc": "36"
                        },
                        "nrCellId": "eFdEDcE7D",
                        "nid": "e5D8B1EbD11"
                    }
                ],
                "tais": [
                    {
                        "plmnId": {
                            "mcc": "585",
                            "mnc": "162"
                        },
                        "tac": "ebef4B",
                        "nid": "fDfC6bbC673"
                    }
```

```
                    ]
                },
                "extraReportReq": {
                    "startTs": "2022-11-23T05:00:30Z",
                    "endTs": "2022-11-30T23:59:59Z"
                },
                "loadLevelThreshold": 0,
                //   default THRESHOLD
                "notificationMethod": "THRESHOLD",
                //   default CROSSED
                "matchingDir": "ASCENDING / DESCENDING / CROSSED",
                "nfLoadLvlThds": null,
                "nfInstanceIds": null,
                "nfSetIds": null,
                "nfTypes": [
                    "SMF"
                ],
                "nsiIdInfos": null,
                "nsiLevelThrds": null,
                "qosRequ": null,
                "qosFlowRetThds": null,
                "ranUeThrouThds": null,
                "repetitionPeriod": 0,
                "snssaia": "N/A",
                "tgtUe": {
                    //   Not applicable to NETWORK_PERFORMANCE
                    "supis": null,
                    "intGroupIds": null,
                    "anyUe": false
                },
                "congThresholds": null,
                //   ----applicable if appIds is provided -----but appIds is not
applicable to NetworkPerformance, so default is not provided in which case
analytics is for overall traffic as per sk3 doc
                "nwPerfRequs": {
                    "nwPerfType": {
                        "GNB_ACTIVE_RATIO": null,
                        "GNB_COMPUTING_USAGE": null,
                        "GNB_MEMORY_USAGE": null,
                        "GNB_DISK_USAGE": null,
                        "NUM_OF_UE": null,
                        "SESS_SUCC_RATIO": null,
                        "HO_SUCC_RATIO": null
                    },
                    // Either "relativeRatio" or "absoluteNum" shall be provided
                    "relativeRatio": null,
                    "absoluteNum": null
                },
                "bwRequs": null,
                "excepRequs": null,
                "exptAnaType": null,
                "exptUeBehav": null
            }
        ],
        //   29.523 - 5.6.2.4
        "evtReq": {
```

```
        "immRep": false,
        // default ON_EVENT_DETECTION
        // If thresholds are defined then ON_EVENT_DETECTION , otherwise
THRESHOLD
        "notifMethod": "ON_EVENT_DETECTION / THRESHOLD",
        "maxReportNbr": 500,
        "monDur": "2022-11-30T23:59:59Z",
        "repPeriod": 10,
        "sampRatio": 75,
        "grpRepTime": 0
    },
    "notificationURI": "http://100.77.47.210:5002/notification",
    //   29.571 - 5.2.2-3
    // as per shared req doc sk3 - 080 for Network Performance
    "supportedFeatures": "080",
    //   applicable if immRep is true
    "eventNotifications": {
        "event": "NETWORK_PERFORMANCE",
        "start": "",
        "expiry": "",
        "timeStampGen": "",
        // If the requested period identified by the "startTs" and "endTs"
attributes in the EventReportingRequirement type is a future time period,
which means the analytics result is a prediction. If no sufficient data is
collected to provide the confidence of the prediction before the time
deadline, the NWDAF shall return a zero confidence
        "nwPerfs": [
            {
                "networkArea": {
                    //   29.554  - 5.6.2.8
                    "ncgis": null,
                    "tais": null
                },
                "nwPerfType": {
                    "GNB_ACTIVE_RATIO": null,
                    "GNB_COMPUTING_USAGE": null,
                    "GNB_MEMORY_USAGE": null,
                    "GNB_DISK_USAGE": null,
                    "NUM_OF_UE": null,
                    "SESS_SUCC_RATIO": null,
                    "HO_SUCC_RATIO": null
                },
                "relativeRatio": null,
                "absoluteNum": null,
                "confidence": null
            }
        ]
    },
    //   Supplied by the NWDAF. When available, shall contain the event(s)
for which the subscription is not successful including the failure reason(s).
    "failEventReports": [
        {
            //   NwdafEvent
            "event": "NETWORK_PERFORMANCE",
            "failureCode": "UNAVAILABLE_DATA / BOTH_STAT_PRED_NOT_ALLOWED /
UNSATISFIED_REQUESTED_ANALYTICS_TIME / OTHER"
```

```
        }
    ],
    //   Either "taiList" or one of "nfId", "nfSetId" shall be provided
    "consNfInfo": {
        "nfId": "uuid",
        "nfSetId": "",
        "taiList": [
            {
                "plmnId": {
                    // TS 38.413
                    "mcc": "",
                    "mnc": ""
                },
                // 38.413
                "tac": ""
            }
        ]
    },
    //  notifCorrId, string, requires support of feature EneNA (seems like
this feature needs to be additionally supported in order to provide
notification correlation id to subscribing NF
    "notifCorrId": null
}
```

Example of the Response Body

```
{
    "eventSubscriptions": [
        {
            "anySlice": "N/A",
            "appIds": null,
            "dnns": null,
            "dnais": null,
            "event": "NETWORK_PERFORMANCE",
            //  necessary for subscribing to AMF  for number of UEs
            "networkArea": //   ---applicable if anyUE:true---
            //   29.554  - 5.6.2.8
            {
                "ncgis": [
                    {
                        "plmnId": {
                            "mcc": "375",
                            "mnc": "36"
                        },
                        "nrCellId": "eFdEDcE7D",
                        "nid": "e5D8B1EbD11"
                    }
                ],
                "tais": [
                    {
                        "plmnId": {
                            "mcc": "585",
                            "mnc": "162"
                        },
                        "tac": "ebef4B",
```

```
                        "nid": "fDfC6bbC673"
                    }
                ]
            },
            "extraReportReq": {
                "startTs": "2022-11-23T05:00:30Z",
                "endTs": "2022-11-30T23:59:59Z"
            },
            "loadLevelThreshold": 0,
            //   default THRESHOLD
            "notificationMethod": "THRESHOLD",
            //   default CROSSED
            "matchingDir": "ASCENDING / DESCENDING / CROSSED",
            "nfLoadLvlThds": null,
            "nfInstanceIds": null,
            "nfSetIds": null,
            "nfTypes": [
                "SMF"
            ],
            "nsiIdInfos": null,
            "nsiLevelThrds": null,
            "qosRequ": null,
            "qosFlowRetThds": null,
            "ranUeThrouThds": null,
            "repetitionPeriod": 0,
            "snssaia": "N/A",
            "tgtUe": {
                //   Not applicable to NETWORK_PERFORMANCE
                "supis": null,
                "intGroupIds": null,
                "anyUe": false
            },
            "congThresholds": null,
            //   ----applicable if appIds is provided -----but appIds is not
applicable to NetworkPerformance, so default is not provided in which case
analytics is for overall traffic as per sk3 doc
            "nwPerfRequs": {
                "nwPerfType": {
                    "GNB_ACTIVE_RATIO": null,
                    "GNB_COMPUTING_USAGE": null,
                    "GNB_MEMORY_USAGE": null,
                    "GNB_DISK_USAGE": null,
                    "NUM_OF_UE": null,
                    "SESS_SUCC_RATIO": null,
                    "HO_SUCC_RATIO": null
                },
                // Either "relativeRatio" or "absoluteNum" shall be provided
                "relativeRatio": null,
                "absoluteNum": null
            },
            "bwRequs": null,
            "excepRequs": null,
            "exptAnaType": null,
            "exptUeBehav": null
        }
    ],
```

```
    //   29.523 - 5.6.2.4
    "evtReq": {
        "immRep": false,
        // default ON_EVENT_DETECTION
        // If thresholds are defined then ON_EVENT_DETECTION , otherwise
THRESHOLD
        "notifMethod": "ON_EVENT_DETECTION / THRESHOLD",
        "maxReportNbr": 500,
        "monDur": "2022-11-30T23:59:59Z",
        "repPeriod": 10,
        "sampRatio": 75,
        "grpRepTime": 0
    },
    "notificationURI": "http://100.77.47.210:5002/notification",
    //   29.571 - 5.2.2-3
    // as per shared req doc sk3 - 080 for Network Performance
    "supportedFeatures": "080",
    //   applicable if immRep is true
    "eventNotifications": {
        "event": "NETWORK_PERFORMANCE",
        "start": "",
        "expiry": "",
        "timeStampGen": "",
        // If the requested period identified by the "startTs" and "endTs"
attributes in the EventReportingRequirement type is a future time period,
which means the analytics result is a prediction. If no sufficient data is
collected to provide the confidence of the prediction before the time
deadline, the NWDAF shall return a zero confidence
        "nwPerfs": [
            {
                "networkArea": {
                    //   29.554  - 5.6.2.8
                    "ncgis": null,
                    "tais": null
                },
                "nwPerfType": {
                    "GNB_ACTIVE_RATIO": null,
                    "GNB_COMPUTING_USAGE": null,
                    "GNB_MEMORY_USAGE": null,
                    "GNB_DISK_USAGE": null,
                    "NUM_OF_UE": null,
                    "SESS_SUCC_RATIO": null,
                    "HO_SUCC_RATIO": null
                },
                "relativeRatio": null,
                "absoluteNum": null,
                "confidence": null
            }
        ]
    },
    //   Supplied by the NWDAF. When available, shall contain the event(s)
for which the subscription is not successful including the failure reason(s).
    "failEventReports": [
        {
            //   NwdafEvent
            "event": "NETWORK_PERFORMANCE",
```

```
            "failureCode": "UNAVAILABLE_DATA / BOTH_STAT_PRED_NOT_ALLOWED /
UNSATISFIED_REQUESTED_ANALYTICS_TIME / OTHER"
        }
    ],
    //   Either "taiList" or one of "nfId", "nfSetId" shall be provided
    "consNfInfo": {
        "nfId": "uuid",
        "nfSetId": "",
        "taiList": [
            {
                "plmnId": {
                    // TS 38.413
                    "mcc": "",
                    "mnc": ""
                },
                // 38.413
                "tac": ""
            }
        ]
    },
    //  notifCorrId, string, requires support of feature EneNA (seems like
this feature needs to be additionally supported in order to provide
notification correlation id to subscribing NF
    "notifCorrId": null
}
```

Modify an existing Network Performance Analytics Subscription

This service operation is used to modify an existing Network Performance Analytics subscription.

Type: PUT

URI: `{apiroot}:{serverPort}:/nnwdaf-eventsubscription/<api version>/subscriptions/{subscriptionId}`

For information on endpoint parameters see, Table 9-16.

Initiated By: Consumers

For information on request body parameters see, Table 9-17

Table 9-22 Supported Response Codes

Code	Description
204	The subscription resource is successfully updated.
400	Bad Request The request is incorrect and subscription is not updated.
500	Indicates a internal server processing error.

Examples

The following example shows how an NF updates a Network Performance Analytics subscription by submitting a PUT request on the REST resource using cURL.

cURL Command

```
curl --location --request PUT '10.123.159.23:8087/nnwdaf-
eventssubscription/v1/subscriptions/371d8527-dcc9-4179-9d67-82e5c93fc206' \
--header 'Content-Type: application/json' \
--data '{
    "notificationURI": "http://prodcon-1:9282/receive",
    "supportedFeatures": "080",
    "eventSubscriptions": [
        {
            "event": "NETWORK_PERFORMANCE",
            "extraReportReq": {
                "startTs": "2023-03-15T18:00:00Z",
                "endTs": "2023-03-16T18:30:00Z",
                "accuracy": null,
                "sampRatio": 70,
                "maxObjectNbr": 5,
                "maxSupiNbr": 2,
                "timeAnaNeeded": null
            },
            "loadLevelThreshold": 1,
            "nfLoadLvlThds": [
                {
                    "congLevel": 20,
                    "nfCpuUsage": 90,
                    "nfLoadLevel": 11,
                    "nfMemoryUsage": 95,
                    "nfStorageUsage": 80
                }
            ],
            "notificationMethod": "THRESHOLD",
            "snssaia": [
                {
                    "sst": 1,
                    "sd": "102030"
                }
            ],
            "tgtUe": {
                "supis": null,
                "intGroupIds": null,
                "anyUe": true
            },
            "nfInstanceIds": null,
            "nfSetIds": null,
            "matchingDir": "CROSSED",
            "networkArea": {
                "ncgis": [
                    {
                        "plmnId": {
                            "mcc": "375",
                            "mnc": "36"
                        },
                        "nrCellId": "0E0FB2773",
                        "nid": "e5D8B1EbD11"
                    }
                ],
```

```
                "tais": [
                    {
                        "plmnId": {
                            "mcc": "585",
                            "mnc": "162"
                        },
                        "tac": "ebef4B",
                        "nid": "fDfC6bbC673"
                    }
                ]
            },
            "nfTypes": [
                "AMF"
            ]
        }
    ],
    "evtReq": {
        "notifMethod": "ONE_TIME",
        "monDur": "2023-04-14T11:10:00Z",
        "immRep": false,
        "maxReportNbr": 2,
        "repPeriod": 1,
        "sampRatio": 70,
        "grpRepTime": 60
    }
}'
```

Example of the Request Body

```
{
    "eventSubscriptions": [
        {
            "anySlice": "N/A",
            "appIds": null,
            "dnns": null,
            "dnais": null,
            "event": "NETWORK_PERFORMANCE",
            //  necessary for subscribing to AMF  for number of UEs
            "networkArea": //   ---applicable if anyUE:true---
            //   29.554  - 5.6.2.8
            {
                "ncgis": [
                    {
                        "plmnId": {
                            "mcc": "375",
                            "mnc": "36"
                        },
                        "nrCellId": "eFdEDcE7D",
                        "nid": "e5D8B1EbD11"
                    }
                ],
                "tais": [
                    {
                        "plmnId": {
                            "mcc": "585",
```

```
                                "mnc": "162"
                            },
                            "tac": "ebef4B",
                            "nid": "fDfC6bbC673"
                        }
                    ]
                },
                "extraReportReq": {
                    "startTs": "2022-11-23T05:00:30Z",
                    "endTs": "2022-11-30T23:59:59Z"
                },
                "loadLevelThreshold": 0,
                //   default THRESHOLD
                "notificationMethod": "THRESHOLD",
                //   default CROSSED
                "matchingDir": "ASCENDING / DESCENDING / CROSSED",
                "nfLoadLvlThds": null,
                "nfInstanceIds": null,
                "nfSetIds": null,
                "nfTypes": [
                    "SMF"
                ],
                "nsiIdInfos": null,
                "nsiLevelThrds": null,
                "qosRequ": null,
                "qosFlowRetThds": null,
                "ranUeThrouThds": null,
                "repetitionPeriod": 0,
                "snssaia": "N/A",
                "tgtUe": {
                    //   Not applicable to NETWORK_PERFORMANCE
                    "supis": null,
                    "intGroupIds": null,
                    "anyUe": false
                },
                "congThresholds": null,
                //   ----applicable if appIds is provided -----but appIds is not
applicable to NetworkPerformance, so default is not provided in which case
analytics is for overall traffic as per sk3 doc
                "nwPerfRequs": {
                    "nwPerfType": {
                        "GNB_ACTIVE_RATIO": null,
                        "GNB_COMPUTING_USAGE": null,
                        "GNB_MEMORY_USAGE": null,
                        "GNB_DISK_USAGE": null,
                        "NUM_OF_UE": null,
                        "SESS_SUCC_RATIO": null,
                        "HO_SUCC_RATIO": null
                    },
                    // Either "relativeRatio" or "absoluteNum" shall be provided
                    "relativeRatio": null,
                    "absoluteNum": null
                },
                "bwRequs": null,
                "excepRequs": null,
                "exptAnaType": null,
```

```
                "exptUeBehav": null
            }
        ],
        //   29.523 - 5.6.2.4
        "evtReq": {
            "immRep": false,
            // default ON_EVENT_DETECTION
            // If thresholds are defined then ON_EVENT_DETECTION , otherwise
    THRESHOLD
            "notifMethod": "ON_EVENT_DETECTION / THRESHOLD",
            "maxReportNbr": 500,
            "monDur": "2022-11-30T23:59:59Z",
            "repPeriod": 10,
            "sampRatio": 75,
            "grpRepTime": 0
        },
        "notificationURI": "http://100.77.47.210:5002/notification",
        //   29.571 - 5.2.2-3
        // as per shared req doc sk3 - 080 for Network Performance
        "supportedFeatures": "080",
        //   applicable if immRep is true
        "eventNotifications": {
            "event": "NETWORK_PERFORMANCE",
            "start": "",
            "expiry": "",
            "timeStampGen": "",
            // If the requested period identified by the "startTs" and "endTs"
    attributes in the EventReportingRequirement type is a future time period,
    which means the analytics result is a prediction. If no sufficient data is
    collected to provide the confidence of the prediction before the time
    deadline, the NWDAF shall return a zero confidence
            "nwPerfs": [
                {
                    "networkArea": {
                        //   29.554  - 5.6.2.8
                        "ncgis": null,
                        "tais": null
                    },
                    "nwPerfType": {
                        "GNB_ACTIVE_RATIO": null,
                        "GNB_COMPUTING_USAGE": null,
                        "GNB_MEMORY_USAGE": null,
                        "GNB_DISK_USAGE": null,
                        "NUM_OF_UE": null,
                        "SESS_SUCC_RATIO": null,
                        "HO_SUCC_RATIO": null
                    },
                    "relativeRatio": null,
                    "absoluteNum": null,
                    "confidence": null
                }
            ]
        },
        //   Supplied by the NWDAF. When available, shall contain the event(s)
    for which the subscription is not successful including the failure reason(s).
        "failEventReports": [
```

```
        {
            //   NwdafEvent
            "event": "NETWORK_PERFORMANCE",
            "failureCode": "UNAVAILABLE_DATA / BOTH_STAT_PRED_NOT_ALLOWED /
UNSATISFIED_REQUESTED_ANALYTICS_TIME / OTHER"
        }
    ],
    //   Either "taiList" or one of "nfId", "nfSetId" shall be provided
    "consNfInfo": {
        "nfId": "uuid",
        "nfSetId": "",
        "taiList": [
            {
                "plmnId": {
                    // TS 38.413
                    "mcc": "",
                    "mnc": ""
                },
                // 38.413
                "tac": ""
            }
        ]
    },
    //  notifCorrId, string, requires support of feature EneNA (seems like
this feature needs to be additionally supported in order to provide
notification correlation id to subscribing NF
    "notifCorrId": null
}
```

Obtain Network Performance Analytics Subscription Information

This service operation is used to obtain information about an existing Network Performance Analytics subscription.

Type: GET

URI: `{apiroot}:{serverPort}:/nnwdaf-eventsubscription/<api version>/subscriptions/{subscriptionId}?event-id={analyticsId}&supported-features={supported-features}&tgt-ue={tgt-ue}&event-filter={event-filter}&ana-req={ana-req}`

For information on endpoint parameters see, Table 9-16.

Initiated By: Consumers

For information on request body parameters see, Table 9-17

Examples

The following example shows how an NF gets subscription information by submitting a GET request on the REST resource using cURL.

cURL Command

```
curl --location 'http://10.123.159.29:8080/nnwdaf-analyticsinfo/v1/analytics?
event-id=NETWORK_PERFORMANCE&supported-features=080&tgt-
ue=%257B%250A%2520%2520%2520%2520%2520%2520%2520%2520%2522supis%2522%253A%2520
null%252C%250A%2520%2520%2520%2520%2520%2520%2520%2520%2522intGroupIds%2522%25
```

```
3A%2520null%252C%250A%2520%2520%2520%2520%2520%2520%2520%2522anyUe%2522%2
53A%2520true%250A%257D&event-
filter=%257B%2522anySlice%2522%253Afalse%252C%2522appIds%2522%253A%255B%2522IQ
PKITNJSE%2522%255D%252C%2522dnns%2522%253A%255B%2522KCRFf30.lafQu2.fOntr02%252
2%255D%252C%2522dnais%2522%253A%255B%2522KuDMa.fDOC%2540DgvaY7.dQUxS69.uTvFz6K
CRFf30.lafQu2.fOntr02%2522%255D%252C%2522networkArea%2522%253A%257B%2522%2522%
253A%255B%257B%2522plmnId%2522%253A%257B%2522mcc%2522%253A%2522611%2522%252C%2
522mnc%2522%253A%2522946%2522%257D%252C%2522eutraCellId%2522%253A%252260De3B8%
2522%252C%2522nid%2522%253A%25222f9CcfeEC9a%2522%257D%255D%252C%2522ncgis%2522
%253A%255B%257B%2522plmnId%2522%253A%257B%2522mcc%2522%253A%2522375%2522%252C%
2522mnc%2522%253A%252236%2522%257D%252C%2522nrCellId%2522%253A%2522eFdEDcE7D%2
522%252C%2522nid%2522%253A%2522e5D8B1EbD11%2522%257D%255D%252C%2522%2522%253A%
255B%257B%2522plmnId%2522%253A%257B%2522mcc%2522%253A%2522791%2522%252C%2522mn
c%2522%253A%2522230%2522%257D%252C%2522n3IwfId%2522%253A%2522CB1E5ba%2522%252C
%2522gNbId%2522%253A%257B%2522bitLength%2522%253A32%252C%2522gNBValue%2522%253
A%2522BF6B9E%2522%257D%252C%2522ngeNbId%2522%253A%2522SMacroNGeNB-
F5CCC%2522%252C%2522wagfId%2522%253A%25228f%2522%252C%2522tngfId%2522%253A%252
21a473d3D%2522%252C%2522nid%2522%253A%2522BFbBAabEBD3%2522%252C%2522eNbId%2522
%253A%2522MacroeNB-
f26ab%2522%257D%255D%252C%2522tais%2522%253A%255B%257B%2522plmnId%2522%253A%25
7B%2522mcc%2522%253A%2522585%2522%252C%2522mnc%2522%253A%2522162%2522%257D%252
C%2522tac%2522%253A%2522ebef4B%2522%252C%2522nid%2522%253A%2522fDfC6bbC673%252
2%257D%255D%257D%252C%2522nwPerfTypes%2522%253A%255B%2522NUM_OF_UE%2522%255D%2
57D&ana-
req=%257B%250A%2520%2520%2520%2520%2522startTs%2522%253A%25222020-07-08T12%253
A00%253A10.000021%2522%252C%250A%2520%2520%2520%2520%2522endTs%2522%253A%25222
021-12-13T12%253A02%253A05.000000%2522%252C%250A%2520%2520%2520%2520%2522timeA
naNeeded%2522%253A%25222022-12-13T12%253A00%253A01.000000%2522%252C%250A%2520%
2520%2520%2520%2522maxObjectNbr%2522%253A0%252C%250A%2520%2520%2520%2520%2522s
ampRatio%2522%253A1%250A%257D'
```

Example of the Response Body

```
{
    "eventSubscriptions": [
        {
            "anySlice": "N/A",
            "appIds": null,
            "dnns": null,
            "dnais": null,
            "event": "NETWORK_PERFORMANCE",
            //  necessary for subscribing to AMF  for number of UEs
            "networkArea": //   ---applicable if anyUE:true---
            //   29.554  - 5.6.2.8
            {
                "ncgis": [
                    {
                        "plmnId": {
                            "mcc": "375",
                            "mnc": "36"
                        },
                        "nrCellId": "eFdEDcE7D",
                        "nid": "e5D8B1EbD11"
                    }
                ],
```

```
                    "tais": [
                        {
                            "plmnId": {
                                "mcc": "585",
                                "mnc": "162"
                            },
                            "tac": "ebef4B",
                            "nid": "fDfC6bbC673"
                        }
                    ]
                },
                "extraReportReq": {
                    "startTs": "2022-11-23T05:00:30Z",
                    "endTs": "2022-11-30T23:59:59Z"
                },
                "loadLevelThreshold": 0,
                //   default THRESHOLD
                "notificationMethod": "THRESHOLD",
                //   default CROSSED
                "matchingDir": "ASCENDING / DESCENDING / CROSSED",
                "nfLoadLvlThds": null,
                "nfInstanceIds": null,
                "nfSetIds": null,
                "nfTypes": [
                    "SMF"
                ],
                "nsiIdInfos": null,
                "nsiLevelThrds": null,
                "qosRequ": null,
                "qosFlowRetThds": null,
                "ranUeThrouThds": null,
                "repetitionPeriod": 0,
                "snssaia": "N/A",
                "tgtUe": {
                    //   Not applicable to NETWORK_PERFORMANCE
                    "supis": null,
                    "intGroupIds": null,
                    "anyUe": false
                },
                "congThresholds": null,
                //   ----applicable if appIds is provided -----but appIds is not
applicable to NetworkPerformance, so default is not provided in which case
analytics is for overall traffic as per sk3 doc
                "nwPerfRequs": {
                    "nwPerfType": {
                        "GNB_ACTIVE_RATIO": null,
                        "GNB_COMPUTING_USAGE": null,
                        "GNB_MEMORY_USAGE": null,
                        "GNB_DISK_USAGE": null,
                        "NUM_OF_UE": null,
                        "SESS_SUCC_RATIO": null,
                        "HO_SUCC_RATIO": null
                    },
                    // Either "relativeRatio" or "absoluteNum" shall be provided
                    "relativeRatio": null,
                    "absoluteNum": null
```

```
            },
            "bwRequs": null,
            "excepRequs": null,
            "exptAnaType": null,
            "exptUeBehav": null
        }
    ],
    //   29.523 - 5.6.2.4
    "evtReq": {
        "immRep": false,
        // default ON_EVENT_DETECTION
        // If thresholds are defined then ON_EVENT_DETECTION , otherwise
THRESHOLD
        "notifMethod": "ON_EVENT_DETECTION / THRESHOLD",
        "maxReportNbr": 500,
        "monDur": "2022-11-30T23:59:59Z",
        "repPeriod": 10,
        "sampRatio": 75,
        "grpRepTime": 0
    },
    "notificationURI": "http://100.77.47.210:5002/notification",
    //   29.571 - 5.2.2-3
    // as per shared req doc sk3 - 080 for Network Performance
    "supportedFeatures": "080",
    //   applicable if immRep is true
    "eventNotifications": {
        "event": "NETWORK_PERFORMANCE",
        "start": "",
        "expiry": "",
        "timeStampGen": "",
        // If the requested period identified by the "startTs" and "endTs"
attributes in the EventReportingRequirement type is a future time period,
which means the analytics result is a prediction. If no sufficient data is
collected to provide the confidence of the prediction before the time
deadline, the NWDAF shall return a zero confidence
        "nwPerfs": [
            {
                "networkArea": {
                    //   29.554  - 5.6.2.8
                    "ncgis": null,
                    "tais": null
                },
                "nwPerfType": {
                    "GNB_ACTIVE_RATIO": null,
                    "GNB_COMPUTING_USAGE": null,
                    "GNB_MEMORY_USAGE": null,
                    "GNB_DISK_USAGE": null,
                    "NUM_OF_UE": null,
                    "SESS_SUCC_RATIO": null,
                    "HO_SUCC_RATIO": null
                },
                "relativeRatio": null,
                "absoluteNum": null,
                "confidence": null
            }
        ]
```

```
    },
    //   Supplied by the NWDAF. When available, shall contain the event(s)
for which the subscription is not successful including the failure reason(s).
    "failEventReports": [
        {
            //   NwdafEvent
            "event": "NETWORK_PERFORMANCE",
            "failureCode": "UNAVAILABLE_DATA / BOTH_STAT_PRED_NOT_ALLOWED /
UNSATISFIED_REQUESTED_ANALYTICS_TIME / OTHER"
        }
    ],
    //   Either "taiList" or one of "nfId", "nfSetId" shall be provided
    "consNfInfo": {
        "nfId": "uuid",
        "nfSetId": "",
        "taiList": [
            {
                "plmnId": {
                    // TS 38.413
                    "mcc": "",
                    "mnc": ""
                },
                // 38.413
                "tac": ""
            }
        ]
    },
    //  notifCorrId, string, requires support of feature EneNA (seems like
this feature needs to be additionally supported in order to provide
notification correlation id to subscribing NF
    "notifCorrId": null
}
```

Delete an existing Network Performance Analytics Subscription

This service operation is used to delete an existing Network Performance Analytics subscription.

Type: DELETE

URI: `{apiroot}:{serverPort}:/nnwdaf-eventsubscription/<api version>/subscriptions/{subscriptionId}`

For information on endpoint parameters see, Table 9-16.

Initiated By: Consumers

Table 9-23 Supported Response Codes

Code	Description
204	The subscription resource is successfully deleted.
404	Not found

The following example shows how an NF deletes subscription information by submitting a DELETE request on the REST resource using cURL.

cURL Command

```
curl --location '10.123.159.23:8087/nnwdaf-eventssubscription/v1/
subscriptions/371d8527-dcc9-4179-9d67-82e5c93fc206'
```

9.3.6 User Data Congestion Analytics APIs

Create a User Data Congestion Analytics Subscription

This service operation is used to create a user data congestion analytics subscription.

Type: POST

URI:`{apiroot}:{serverPort}:/nnwdaf-eventsubscription/<api version>/subscriptions`

Table 9-24 Endpoint Parameters

Parameter	Description	Example
`{apiroot}`	The IP used to access the OCNWDAF subscription.	
`{serverport}`	The port used to access the OCNWDAF subscription. Default value is 8080.	
`{subscriptionId}`	Subscription ID	
`{analyticsId}`	The analytics ID is "USER_DATA_CONGESTION"	
`{supported-features}`	020	
`{tgt-ue}`	Encoded Target UE information.	`{ "supis": null, "intGroupIds": null, "anyUe": true }`

Table 9-24 (Cont.) Endpoint Parameters

Parameter	Description	Example
{event-filter}	Encoded event filter value.	{ "anySlice": false, "networkArea": { "ecgis": [{ "plmnId": { "mcc": "611", "mnc": "946" }, "eutraCellId": "60De3B8", "nid": "2f9CcfeEC9a" }], "ncgis": [{ "plmnId": { "mcc": "375", "mnc": "36" }, "nrCellId": "eFdEDcE7D",

Table 9-24 (Cont.) Endpoint Parameters

Parameter	Description	Example
		<pre>"nid": "e5D8B1EbD11" }], "tais": [{ "plmnId": { "mcc": "585", "mnc": "162" }, "tac": "ebef4B", "nid": "fDfC6bbC673" }] }, "nwPerfTypes": ["NUM_OF_UE"] }</pre>

Table 9-24 (Cont.) Endpoint Parameters

Parameter	Description	Example

{ana-req}	Encoded value of analytics requirements.	{
		
		"startTs":"2023-02-08T12:00:10.000021",
		
		"endTs":"2023-05-13T12:02:05.000000",
		
		"timeAnaNeeded":"2024-12-13T12:00:01.000000",
		
		"maxObjectNbr":10,
		
		"sampRatio":1
		
		}

Initiated By: Consumers

Request Body Parameters

Table 9-25 Type NnwdafEventsSubscription

Parameter	Data Type	Presence	Description
eventSubscriptions	array(EventSubscription)	M	Subscribed events. The event parameter within event subscriptions is "USER DATA CONGESTION".
evtReq	ReportingInformation	O	Represents the reporting requirements of the event subscription. If this parameter is not given then the default values for ReportingInformation is used. The notification method "notifMethod" within ReportingInformation takes precedence over notificationMethod within EventSubscription.
notificationURI	URI	C	URI to which the OCNWDAF sends the reports.

Table 9-25 (Cont.) Type NnwdafEventsSubscription

Parameter	Data Type	Presence	Description
eventNotifications	array(EventNotification)	C	Notifications about Individual Events. Present only if the immediate reporting indication in the "immRep" attribute within the "evtReq" attribute is set to true in the event subscription, and the reports are available. Present in the response to OCNWDAF subscription if "immRep" is true and the reports are the available.
failEventReports	array(FailureEventInfo)	O	Supplied by the OCNWDAF. When this parameter is available, it contains the event(s) for which the subscription is not successful including the failure reason(s). This parameter is populated and returned in response to the error case.
consNfInfo	ConsumerNfInformation	O	Represents the analytics consumer NF information.
notifCorrId	String	M	Notification correlation ID. It is generated after a successful subscription and is returned in the response.
supportedFeatures	SupportedFeatures	C	This parameter is supplied by NF service consumer in the POST request for OCNWDAF Event Subscriptions resource creation, and sent by the OCNWDAF in the corresponding response. Value is "020" for User Data Congestion ID.

Table 9-26 Type EventSubscription

Parameter	Data Type	Presence	Description
anySlice	AnySlice	M	Represents the any slice.
appIds	array(ApplicationId)	C	**Note:** This parameter is not applicable for user data congestion analytics.
dnns	array(Dnn)	C	**Note:** This parameter is not applicable for user data congestion analytics.
dnais	array(Dnai)	C	**Note:** This parameter is not applicable for user data congestion analytics.

Table 9-26 (Cont.) Type EventSubscription

Parameter	Data Type	Presence	Description
event	NwdafEvent	M	Indicates the subscribed event. The value for user data congestion analytics is "USER DATA CONGESTION".
extraReportReq	EventReportingRequirement	O	The additional event reporting requirements information.
ladnDnns	array(Dnn)	M	**Note:** This parameter is not applicable for user data congestion analytics.
matchingDir	MatchingDirection	O	A matching direction can be provided along with a threshold. If this parameter is omitted, the default value is CROSSED.
nfLoadLvlThds	array(ThresholdLevel)	C	**Note:** This parameter is not applicable for user data congestion analytics.
networkArea	NetworkAreaInfo	C	Identification of network area to which the subscription applies. The absence of networkArea means subscription to all network areas.
visitedAreas	array(NetworkAreaInfo)	O	**Note:** This parameter is not applicable for user data congestion analytics.
maxTopAppUlNbr	Uinteger		**Note:** This parameter is not applicable for user data congestion analytics.
maxTopAppDlNbr	Uinteger		**Note:** This parameter is not applicable for user data congestion analytics.
nfInstanceIds	array(NfInstanceId)		**Note:** This parameter is not applicable for user data congestion analytics.
nfSetIds	array(NfSetId)		**Note:** This parameter is not applicable for user data congestion analytics.
nfTypes	array(NFType)		**Note:** This parameter is not applicable for user data congestion analytics.

Table 9-26 (Cont.) Type EventSubscription

Parameter	Data Type	Presence	Description
notificationMethod	NotificationMethod	O	Indicates the notification method.
nsiIdInfos	array(NsiIdInfo)	O	**Note:** This parameter is not applicable for user data congestion analytics.
nsiLevelThrds	array(Uinteger)	O	**Note:** This parameter is not applicable for user data congestion analytics.
qosRequ	QosRequirement	C	**Note:** This parameter is not applicable for user data congestion analytics.
qosFlowRetThds	array(RetainabilityThreshold)	C	**Note:** This parameter is not applicable for user data congestion analytics.
ranUeThrouThds	array(BitRate)	C	**Note:** This parameter is not applicable for user data congestion analytics.
repetitionPeriod	DurationSec	C	This parameter is provided by the "notificationMethod" attribute if the notification method is "PERIODIC".
snssais	array(Snssai)	C	Identification(s) of network slice to which the subscription applies. **Note:** This parameter is not applicable for user data congestion analytics.
tgtUe	TargetUeInformation	O	Identifies target the UE information.
congThresholds	array(ThresholdLevel)	C	This parameter identifies the congestion thresholds for user data congestion analytics.
nwPerfRequs	array(NetworkPerfRequirement)	C	**Note:** This parameter is not applicable for user data congestion analytics.
bwRequs	array(BwRequirement)	O	**Note:** This parameter is not applicable for user data congestion analytics.

Table 9-26 (Cont.) Type EventSubscription

Parameter	Data Type	Presence	Description
excepRequs	array(Exception)	C	**Note:** This parameter is not applicable for user data congestion analytics.
exptAnaType	ExpectedAnalyticsType	C	**Note:** This parameter is not applicable for user data congestion analytics.
exptUeBehav	ExpectedUeBehaviourData	O	**Note:** This parameter is not applicable for user data congestion analytics.
ratFreqs	array(RatFreqInformation)	O	**Note:** This parameter is not applicable for user data congestion analytics.
listOfAnaSubsets	array(AnalyticsSubset)	O	**Note:** This parameter is not applicable for user data congestion analytics.
disperReqs	array(DispersionRequirement)	O	**Note:** This parameter is not applicable for user data congestion analytics.
redTransReqs	array(RedundantTransmissionExpReq)	O	**Note:** This parameter is not applicable for user data congestion analytics.
wlanReqs	array(WlanPerformanceReq)	O	**Note:** This parameter is not applicable for user data congestion analytics.
upfInfo	UpfInformation	O	**Note:** This parameter is not applicable for user data congestion analytics.
appServerAddrs	array(AddrFqdn)	C	**Note:** This parameter is not applicable for user data congestion analytics.
dnPerfReqs	array(DnPerformanceReq)	O	**Note:** This parameter is not applicable for user data congestion analytics.

Table 9-27 Type NnwdafEventsSubscriptionNotification

Parameter	Data Type	Presence	Description
eventNotifications	array (EventNotification)	C	Notifications about individual events.

Table 9-27 (Cont.) Type NnwdafEventsSubscriptionNotification

Parameter	Data Type	Presence	Description
subscriptionId	String	M	String identifying a subscription to the Nnwdaf_EventsSubscription service.
notifCorrId	String	O	**Note:** This parameter is not applicable for user data congestion analytics.
oldSubscriptionId	String	C	**Note:** This parameter is not applicable for user data congestion analytics.
resourceUri	URI	C	**Note:** This parameter is not applicable for user data congestion analytics.
termCause	TermCause	O	**Note:** This parameter is not applicable for user data congestion analytics.

Table 9-28 Type EventNotification

Parameter	Data Type	Presence	Description
event	NwdafEvent	M	Subscribed events. The event parameter within event Subscriptions has to be "USER_DATA_CONGESTION"
start	DateTime	O	It defines the start time from when the analytics information becomes valid.
expiry	DateTime	O	It defines the expiration time after which the analytics information will become invalid.
timeStampGen	DateTime	C	It defines the timestamp of analytics generation.
failNotifyCode	NwdafFailureCode	C	**Note:** This parameter is not applicable for user data congestion analytics.
rvWaitTime	DurationSec	O	**Note:** This parameter is not applicable for user data congestion analytics.

Table 9-28 (Cont.) Type EventNotification

Parameter	Data Type	Presence	Description
anaMetaInfo	AnalyticsMetadataInfo	C	**Note:** This parameter is not applicable for user data congestion analytics.
nwPerfs	array(NetworkPerfInfo)	C	**Note:** This parameter is not applicable for user data congestion analytics.
nfLoadLevelInfos	array(NfLoadLevelInformation)	C	**Note:** This parameter is not applicable for user data congestion analytics.
nsiLoadLevelInfos	array(NsiLoadLevelInfo)	C	**Note:** This parameter is not applicable for user data congestion analytics.
qosSustainInfos	array(QosSustainabilityInfo)	C	**Note:** This parameter is not applicable for user data congestion analytics.
sliceLoadLevelInfo	SliceLoadLevelInformation	C	**Note:** This parameter is not applicable for user data congestion analytics.
svcExps	array(ServiceExperienceInfo)		**Note:** This parameter is not applicable for user data congestion analytics.
ueComms	array(UeCommunication)	C	**Note:** This parameter is not applicable for user data congestion analytics.
ueMobs	array(UeMobility)	C	**Note:** This parameter is not applicable for user data congestion analytics.
abnorBehavrs	array(AbnormalBehaviour)	C	**Note:** This parameter is not applicable for user data congestion analytics.
userDataCongInfos	array(UserDataCongestionInfo)	C	The User Data Congestion information.
dnPerfInfos	array(DnPerfInfo)	C	**Note:** This parameter is not applicable for user data congestion analytics.
disperInfos	array(DispersionInfo)	C	**Note:** This parameter is not applicable for user data congestion analytics.

Table 9-28 (Cont.) Type EventNotification

Parameter	Data Type	Presence	Description
redTransInfos	array(RedundantTransmissionExpInfo)	C	**Note:** This parameter is not applicable for user data congestion analytics.
wlanInfos	array(WlanPerformanceInfo)	C	**Note:** This parameter is not applicable for user data congestion analytics.
smccExps	array(SmcceInfo)	C	**Note:** This parameter is not applicable for user data congestion analytics.

Table 9-29 Type EventNotification

Parameter	Data Type	Presence	Description
start	DateTime	O	It defines the start time from when the analytics information becomes valid.
expiry	DateTime	O	It defines the expiration time after which the analytics information will become invalid.
timeStampGen	DateTime	C	It defines the timestamp of analytics generation.
anaMetaInfo	AnalyticsMetadataInfo	C	**Note:** This parameter is not applicable for user data congestion analytics.
sliceLoadLevelInfos	array(SliceLoadLevelInformation)	C	**Note:** This parameter is not applicable for user data congestion analytics.
nsiLoadLevelInfos	array(NsiLoadLevelInfo)	C	**Note:** This parameter is not applicable for user data congestion analytics.
nwPerfs	array(NetworkPerfInfo)	C	**Note:** This parameter is not applicable for user data congestion analytics.
nfLoadLevelInfos	array(NfLoadLevelInformation)	C	**Note:** This parameter is not applicable for user data congestion analytics.
qosSustainInfos	array(QosSustainabilityInfo)	C	**Note:** This parameter is not applicable for user data congestion analytics.

Table 9-29 (Cont.) Type EventNotification

Parameter	Data Type	Presence	Description
ueMobs	array(UeMobility)	C	**Note:** This parameter is not applicable for user data congestion analytics.
ueComms	array(UeCommunication)	C	**Note:** This parameter is not applicable for user data congestion analytics.
userDataCongInfos	array(UserDataCongestionInfo)	C	The notification information for User Data Congestion.
suppFeat	SupportedFeatures	C	**Note:** This parameter is not applicable for user data congestion analytics.
svcExps	array(ServiceExperienceInfo)	C	**Note:** This parameter is not applicable for user data congestion analytics.
abnorBehavrs	array(AbnormalBehaviour)	C	**Note:** This parameter is not applicable for user data congestion analytics.
smccExps	array(SmcceInfo)	C	**Note:** This parameter is not applicable for user data congestion analytics.
disperInfos	array(DispersionInfo)	C	**Note:** This parameter is not applicable for user data congestion analytics.
redTransInfos	array(RedundantTransmissionExpInfo)	C	**Note:** This parameter is not applicable for user data congestion analytics.
wlanInfos	array(WlanPerformanceInfo)	C	**Note:** This parameter is not applicable for user data congestion analytics.
dnPerfInfos	array(DnPerfInfo)	C	**Note:** This parameter is not applicable for user data congestion analytics.

Table 9-30 Supported Response Codes

Code	Description
201	The subscription is created successfully.
400	Bad Request. The request is incorrect and subscription is not created.

Table 9-30 (Cont.) Supported Response Codes

Code	Description
500	Indicates a internal server processing error.

Examples

The following example shows how an NF creates a subscription for user data congestion analytics by submitting a POST request on the REST resource using cURL.

cURL Command

```
curl --location '10.123.159.23:8087/nnwdaf-eventssubscription/v1/
subscriptions' \
--header 'accept: application/json' \
--header 'Content-Type: application/json' \
--data '{
    "notificationURI": "http://prodcon-1:9282/receive",
    "supportedFeatures": "020",
    "eventSubscriptions": [
        {
            "event": "USER_DATA_CONGESTION",
            "extraReportReq": {
                "startTs": "2023-07-17T10:00:00Z",
                "endTs": "2023-07-17T11:00:00Z",
                "accuracy": null,
                "sampRatio": 70,
                "maxObjectNbr": 5,
                "maxSupiNbr": 2,
                "timeAnaNeeded": null
            },
            "notificationMethod": null,
            "congThresholds": [{
                "congLevel": 10,
                "nfLoadLevel": null,
                "nfCpuUsage": null,
                "nfMemoryUsage": null,
                "nfStorageUsage": null,
                "avgTrafficRate": null,
                "avgPacketDelay": null,
                "maxPacketDelay": null,
                "avgPacketLossRate": null,
                "svcExpLevel": null
            }],
            "tgtUe": {
                "supis": null,
                "intGroupIds": null,
                "anyUe": true
            },
            "nfInstanceIds": null,
            "nfSetIds": null,
            "matchingDir": "ASCENDING",
            "snssais": [
                {
```

```
                    "sst": 1,
                    "sd": "104030"
                }
            ],
            "networkArea": {
                "ecgis": [
                    {
                        "plmnId": {
                            "mcc": "611",
                            "mnc": "946"
                        },
                        "eutraCellId": "60De3B8",
                        "nid": "2f9CcfeEC9a"
                    }
                ],
                "ncgis": [
                    {
                        "plmnId": {
                            "mcc": "375",
                            "mnc": "36"
                        },
                        "nrCellId": "27C042641",
                        "nid": "e5D8B1EbD11"
                    }
                ],
                "tais": [
                    {
                        "plmnId": {
                            "mcc": "585",
                            "mnc": "162"
                        },
                        "tac": "ebef4B",
                        "nid": "fDfC6bbC673"
                    }
                ]
            },
        }
    ],
    "evtReq": {
        "notifMethod": "ONE_TIME",
        "monDur": "2023-07-17T12:25:00Z",
        "immRep": false,
        "maxReportNbr": 2,
        "repPeriod": 1,
        "sampRatio": 70,
        "grpRepTime": 60
    }
}
```

Example of the Request Body

```
{
    "notificationURI": "http://prodcon-1:9282/receive",
    "supportedFeatures": "020",
    "eventSubscriptions": [
```

```
{
    "event": "USER_DATA_CONGESTION",
    "extraReportReq": {
        "startTs": "2023-07-17T10:00:00Z",
        "endTs": "2023-07-17T11:00:00Z",
        "accuracy": null,
        "sampRatio": 70,
        "maxObjectNbr": 5,
        "maxSupiNbr": 2,
        "timeAnaNeeded": null
    },
    "notificationMethod": null,
    "congThresholds": [{
        "congLevel": 10,
        "nfLoadLevel": null,
        "nfCpuUsage": null,
        "nfMemoryUsage": null,
        "nfStorageUsage": null,
        "avgTrafficRate": null,
        "avgPacketDelay": null,
        "maxPacketDelay": null,
        "avgPacketLossRate": null,
        "svcExpLevel": null
    }],
    "tgtUe": {
        "supis": null,
        "intGroupIds": null,
        "anyUe": true
    },
    "nfInstanceIds": null,
    "nfSetIds": null,
    "matchingDir": "ASCENDING",
    "snssais": [
        {
            "sst": 1,
            "sd": "104030"
        }
    ],
    "networkArea": {
        "ecgis": [
            {
                "plmnId": {
                    "mcc": "611",
                    "mnc": "946"
                },
                "eutraCellId": "60De3B8",
                "nid": "2f9CcfeEC9a"
            }
        ],
        "ncgis": [
            {
                "plmnId": {
                    "mcc": "375",
                    "mnc": "36"
                },
                "nrCellId": "27C042641",
```

```
                        "nid": "e5D8B1EbD11"
                    }
                ],
                "tais": [
                    {
                        "plmnId": {
                            "mcc": "585",
                            "mnc": "162"
                        },
                        "tac": "ebef4B",
                        "nid": "fDfC6bbC673"
                    }
                ]
            },
             ]
        }
    ],
    "evtReq": {
        "notifMethod": "ONE_TIME",
        "monDur": "2023-07-17T12:25:00Z",
        "immRep": false,
        "maxReportNbr": 2,
        "repPeriod": 1,
        "sampRatio": 70,
        "grpRepTime": 60
    }
}
```

Example of the Response Body

```
{
    "eventSubscriptions": [
        {
            "event": "USER_DATA_CONGESTION",
            "extraReportReq": {
                "startTs": "2023-07-17T10:00:00Z",
                "endTs": "2023-07-17T11:00:00Z",
                "sampRatio": 70,
                "maxObjectNbr": 5,
                "maxSupiNbr": 2
            },
            "matchingDir": "ASCENDING",
            "networkArea": {
                "ecgis": [
                    {
                        "plmnId": {
                            "mcc": "611",
                            "mnc": "946"
                        },
                        "eutraCellId": "60De3B8",
                        "nid": "2f9CcfeEC9a"
                    }
                ],
                "ncgis": [
                    {
```

```
                            "plmnId": {
                                "mcc": "375",
                                "mnc": "36"
                            },
                            "nrCellId": "27C042641",
                            "nid": "e5D8B1EbD11"
                        }
                    ],
                    "tais": [
                        {
                            "plmnId": {
                                "mcc": "585",
                                "mnc": "162"
                            },
                            "tac": "ebef4B",
                            "nid": "fDfC6bbC673"
                        }
                    ]
                },
                "snssais": [
                    {
                        "sst": 1,
                        "sd": "104030"
                    }
                ],
                "tgtUe": {
                    "anyUe": true
                },
                "congThresholds": [
                    {
                        "congLevel": 10
                    }
                ]
            }
        ],
        "evtReq": {
            "immRep": false,
            "notifMethod": "ONE_TIME",
            "maxReportNbr": 2,
            "monDur": "2023-08-02T06:37:00Z",
            "repPeriod": 1,
            "sampRatio": 70,
            "grpRepTime": 60
        },
        "notificationURI": "http://prodcon-1:9282/receive",
        "notifCorrId": "c7e20068-fc61-45f9-87bb-ea6ecd4b27a0",
        "supportedFeatures": "020"
}
```


Modify an Existing User Data Congestion Analytics Subscription

This service operation is used to modify an existing User Data Congestion Analytics subscription.

Type: PUT

URI: `{apiroot}:{serverPort}:/nnwdaf-eventsubscription/<api version>/subscriptions/{subscriptionId}`

For information on endpoint parameters see, Table 9-24.

Initiated By: Consumers

For information on request body parameters see, Table 9-25

Table 9-31 Supported Response Codes

Code	Description
204	The subscription resource is successfully updated.
400	Bad Request The request is incorrect and subscription is not updated.
500	Indicates a internal server processing error.

Examples

The following example shows how an NF updates a User Data Congestion Analytics subscription by submitting a PUT request on the REST resource using cURL.

cURL Command

```
curl --location --request PUT '10.123.159.23:8087/nnwdaf-
eventssubscription/v1/subscriptions/371d8527-dcc9-4179-9d67-82e5c93fc206' \
--header 'Content-Type: application/json' \
--data '
{
    "notificationURI": "http://prodcon-1:9282/receive",
    "supportedFeatures": "020",
    "eventSubscriptions": [
        {
            "event": "USER_DATA_CONGESTION",
            "extraReportReq": {
                "startTs": "2023-07-17T10:00:00Z",
                "endTs": "2023-07-17T11:00:00Z",
                "accuracy": null,
                "sampRatio": 70,
                "maxObjectNbr": 5,
                "maxSupiNbr": 2,
                "timeAnaNeeded": null
            },
            "notificationMethod": null,
            "congThresholds": [{
                "congLevel": 10,
                "nfLoadLevel": null,
                "nfCpuUsage": null,
                "nfMemoryUsage": null,
                "nfStorageUsage": null,
                "avgTrafficRate": null,
                "avgPacketDelay": null,
                "maxPacketDelay": null,
                "avgPacketLossRate": null,
                "svcExpLevel": null
            }],
```

```
            "tgtUe": {
                "supis": null,
                "intGroupIds": null,
                "anyUe": true
            },
            "nfInstanceIds": null,
            "nfSetIds": null,
            "matchingDir": "ASCENDING",
            "snssais": [
                {
                    "sst": 1,
                    "sd": "104030"
                }
            ],
            "networkArea": {
                "ecgis": [
                    {
                        "plmnId": {
                            "mcc": "611",
                            "mnc": "946"
                        },
                        "eutraCellId": "60De3B8",
                        "nid": "2f9CcfeEC9a"
                    }
                ],
                "ncgis": [
                    {
                        "plmnId": {
                            "mcc": "375",
                            "mnc": "36"
                        },
                        "nrCellId": "27C042641",
                        "nid": "e5D8B1EbD11"
                    }
                ],
                "tais": [
                    {
                        "plmnId": {
                            "mcc": "585",
                            "mnc": "162"
                        },
                        "tac": "ebef4B",
                        "nid": "fDfC6bbC673"
                    }
                ]
            },
        }
    ],
    "evtReq": {
        "notifMethod": "ONE_TIME",
        "monDur": "2023-07-17T12:25:00Z",
        "immRep": false,
        "maxReportNbr": 2,
        "repPeriod": 1,
        "sampRatio": 70,
        "grpRepTime": 60
```

```
    }
}
```

Example of the Request Body

```
{
    "notificationURI": "http://prodcon-1:9282/receive",
    "supportedFeatures": "020",
    "eventSubscriptions": [
        {
            "event": "USER_DATA_CONGESTION",
            "extraReportReq": {
                "startTs": "2023-07-17T10:00:00Z",
                "endTs": "2023-07-17T11:00:00Z",
                "accuracy": null,
                "sampRatio": 70,
                "maxObjectNbr": 5,
                "maxSupiNbr": 2,
                "timeAnaNeeded": null
            },
            "notificationMethod": null,
            "congThresholds": [{
                "congLevel": 10,
                "nfLoadLevel": null,
                "nfCpuUsage": null,
                "nfMemoryUsage": null,
                "nfStorageUsage": null,
                "avgTrafficRate": null,
                "avgPacketDelay": null,
                "maxPacketDelay": null,
                "avgPacketLossRate": null,
                "svcExpLevel": null
            }],
            "tgtUe": {
                "supis": null,
                "intGroupIds": null,
                "anyUe": true
            },
            "nfInstanceIds": null,
            "nfSetIds": null,
            "matchingDir": "ASCENDING",
            "snssais": [
                {
                    "sst": 1,
                    "sd": "104030"
                }
            ],
            "networkArea": {
                "ecgis": [
                    {
                        "plmnId": {
                            "mcc": "611",
                            "mnc": "946"
                        },
                        "eutraCellId": "60De3B8",
```

```
                        "nid": "2f9CcfeEC9a"
                    }
                ],
                "ncgis": [
                    {
                        "plmnId": {
                            "mcc": "375",
                            "mnc": "36"
                        },
                        "nrCellId": "27C042641",
                        "nid": "e5D8B1EbD11"
                    }
                ],
                "tais": [
                    {
                        "plmnId": {
                            "mcc": "585",
                            "mnc": "162"
                        },
                        "tac": "ebef4B",
                        "nid": "fDfC6bbC673"
                    }
                ]
            },
        }
    ],
    "evtReq": {
        "notifMethod": "ONE_TIME",
        "monDur": "2023-07-17T12:25:00Z",
        "immRep": false,
        "maxReportNbr": 2,
        "repPeriod": 1,
        "sampRatio": 70,
        "grpRepTime": 60
    }
}
```


Obtain User Data Congestion Analytics Subscription Information

This service operation is used to obtain information about an existing User Data Congestion Analytics subscription.

Type: GET

URI: `{apiroot}:{serverPort}:/nnwdaf-eventsubscription/<api version>/subscriptions/{subscriptionId}?event-id={analyticsId}&supported-features={supported-features}&tgt-ue={tgt-ue}&event-filter={event-filter}&ana-req={ana-req}`

For information on endpoint parameters see, Table 9-24 .

Initiated By: Consumers

For information on request body parameters see, Table 9-25

Examples

The following example shows how an NF gets subscription information by submitting a GET request on the REST resource using cURL.

cURL Command

```
curl --location 'http://10.123.159.29:8080/nnwdaf-analyticsinfo/v1/analytics?
event-id=USER_DATA_CONGESTION&supported-features=020&tgt-
ue=%257B%250A%2520%2520%2520%2520%2520%2520%2520%2520%2522supis%2522%253A%2520
null%252C%250A%2520%2520%2520%2520%2520%2520%2520%2520%2522intGroupIds%2522%25
3A%2520null%252C%250A%2520%2520%2520%2520%2520%2520%2520%2520%2522anyUe%2522%2
53A%2520true%250A%257D&event-
filter=%257B%2522anySlice%2522%253Afalse%252C%2522appIds%2522%253A%255B%2522IQ
PKITNJSE%2522%255D%252C%2522dnns%2522%253A%255B%2522KCRFf30.lafQu2.fOntr02%252
2%255D%252C%2522dnais%2522%253A%255B%2522KuDMa.fDOC%2540DgvaY7.dQUxS69.uTvFz6K
CRFf30.lafQu2.fOntr02%2522%255D%252C%2522networkArea%2522%253A%257B%2522ecgis%
2522%253A%255B%257B%2522plmnId%2522%253A%257B%2522mcc%2522%253A%2522611%2522%2
52C%2522mnc%2522%253A%2522946%2522%257D%252C%2522eutraCellId%2522%253A%252260D
e3B8%2522%252C%2522nid%2522%253A%25222f9CcfeEC9a%2522%257D%255D%252C%2522ncgis
%2522%253A%255B%257B%2522plmnId%2522%253A%257B%2522mcc%2522%253A%2522375%2522%
252C%2522mnc%2522%253A%252236%2522%257D%252C%2522nrCellId%2522%253A%2522eFdEDc
E7D%2522%252C%2522nid%2522%253A%2522e5D8B1EbD11%2522%257D%255D%252C%2522plmnId
%2522%253A%257B%2522mcc%2522%253A%2522791%2522%252C%2522mnc%2522%253A%2522230%
2522%257D%252C%2522n3IwfId%2522%253A%2522CB1E5ba%2522%252C%2522gNbId%2522%253A
%257B%2522bitLength%2522%253A32%252C%2522gNBValue%2522%253A%2522BF6B9E%2522%25
7D%252C%2522ngeNbId%2522%253A%2522SMacroNGeNB-
F5CCC%2522%252C%2522wagfId%2522%253A%25228f%2522%252C%2522tngfId%2522%253A%252
21a473d3D%2522%252C%2522nid%2522%253A%2522BFbBAabEBD3%2522%252C%2522eNbId%2522
%253A%2522MacroeNB-
f26ab%2522%257D%255D%252C%2522tais%2522%253A%255B%257B%2522plmnId%2522%253A%25
7B%2522mcc%2522%253A%2522585%2522%252C%2522mnc%2522%253A%2522162%2522%257D%252
C%2522tac%2522%253A%2522ebef4B%2522%252C%2522nid%2522%253A%2522fDfC6bbC673%252
2%257D%255D%257D%252C%2522nwPerfTypes%2522%253A%255B%2522NUM_OF_UE%2522%255D%2
57D&ana-
req=%257B%250A%2520%2520%2520%2520%2522startTs%2522%253A%25222020-07-08T12%253
A00%253A10.000021%2522%252C%250A%2520%2520%2520%2520%2522endTs%2522%253A%25222
021-12-13T12%253A02%253A05.000000%2522%252C%250A%2520%2520%2520%2520%2522timeA
naNeeded%2522%253A%25222022-12-13T12%253A00%253A01.000000%2522%252C%250A%2520%
2520%2520%2520%2522maxObjectNbr%2522%253A0%252C%250A%2520%2520%2520%2520%2522s
ampRatio%2522%253A1%250A%257D'
```

Example of the Response Body

```
{
    "eventSubscriptions": [
        {
            "event": "USER_DATA_CONGESTION",
            "extraReportReq": {
                "startTs": "2023-07-17T10:00:00Z",
                "endTs": "2023-07-17T11:00:00Z",
                "sampRatio": 70,
                "maxObjectNbr": 5,
                "maxSupiNbr": 2
            },
```

```
            "matchingDir": "ASCENDING",
            "networkArea": {
                "ecgis": [
                    {
                        "plmnId": {
                            "mcc": "611",
                            "mnc": "946"
                        },
                        "eutraCellId": "60De3B8",
                        "nid": "2f9CcfeEC9a"
                    }
                ],
                "ncgis": [
                    {
                        "plmnId": {
                            "mcc": "375",
                            "mnc": "36"
                        },
                        "nrCellId": "27C042641",
                        "nid": "e5D8B1EbD11"
                    }
                ],
                "tais": [
                    {
                        "plmnId": {
                            "mcc": "585",
                            "mnc": "162"
                        },
                        "tac": "ebef4B",
                        "nid": "fDfC6bbC673"
                    }
                ]
            },
            "snssais": [
                {
                    "sst": 1,
                    "sd": "104030"
                }
            ],
            "tgtUe": {
                "anyUe": true
            },
            "congThresholds": [
                {
                    "congLevel": 10
                }
            ]
        }
    ],
    "evtReq": {
        "immRep": false,
        "notifMethod": "ONE_TIME",
        "maxReportNbr": 2,
        "monDur": "2023-08-02T06:37:00Z",
        "repPeriod": 1,
        "sampRatio": 70,
```

```
        "grpRepTime": 60
    },
    "notificationURI": "http://prodcon-1:9282/receive",
    "notifCorrId": "c7e20068-fc61-45f9-87bb-ea6ecd4b27a0",
    "supportedFeatures": "020"
}
```

Delete an Existing User Data Congestion Analytics Subscription

This service operation is used to delete an existing User Data Congestion Analytics subscription.

Type: DELETE

URI: `{apiroot}:{serverPort}:/nnwdaf-eventsubscription/<api version>/subscriptions/{subscriptionId}`

For information on endpoint parameters see, Table 9-24.

Initiated By: Consumers

Table 9-32 Supported Response Codes

Code	Description
204	The subscription resource is successfully deleted.
404	Not found

The following example shows how an NF deletes subscription information by submitting a DELETE request on the REST resource using cURL.

cURL Command

```
curl --location '10.123.159.23:8087/nnwdaf-eventssubscription/v1/subscriptions/371d8527-dcc9-4179-9d67-82e5c93fc206'
```

9.3.7 QoS Sustainability Analytics APIs

QoS Sustainability Analytics Rest API Parameters

> **Note**
>
> The data types supported by OCNWDAF comply with the 3GPP specifications. For more information about the 3GPP data types, see 3GPP Technical Specification 29.520, Release 17, Network Data Analytics Services.

Request Parameters

Listed below are the QoS sustainability analytics request parameters:

Table 9-33 Request Parameters

Parameter	Data Type	Presence	Description
eventSubscriptions	EventSubscription	M	Specifies the subscribed event. The event parameter within the subscription is set to "QOS SUSTAINABILITY".
evtReq	ReportingInformation	O	Represents the reporting requirements of the event subscription. If this parameter is not provided, the default values for *ReportingInformation* is used. The notification method "notifMethod" within *ReportingInformation* takes precedence over the *notificationMethod* within *EventSubscription*.
notificationURI	Uri	C	The URI to which OCNWDAF sends the reports
eventNotifications	array	C	Notifications about individual events This parameter is present if the immediate reporting indication in the "*immRep*" attribute within the "*evtReq*" attribute is set to true in the event subscription and the reports are available. This parameter is provided in response to the OCNWDAF subscription if *immediatereport* is true and the reports are available.

Table 9-33 (Cont.) Request Parameters

Parameter	Data Type	Presence	Description
failEventReports	array	O	This parameter is provided by the OCNWDAF. When this parameter is available, it contains the event(s) for which the subscription is not successful, it also includes the failure reason(s). This parameter is populated and returned in the response for the error case.
consNfInfo	ConsumerNfInformation	O	Represents the analytics consumer NF information
notifCorrId	String	M	Notification correlation identifier. It is generated after a successful subscription and is returned in the response.
supportedFeatures	SupportedFeatures	C	This parameter is provided by the NF service consumer in the POST request for creating an OCNWDAF Event Subscription resource, and it is also provided in response to the corresponding request.

Table 9-34 EventSubscription

Parameter	Data Type	Presence	Description
anySlice	AnySlice	M	Represents the any slice. Default is FALSE.
appIds	array	C	**Note:** This parameter is not applicable for QoS sustainability analytics.
dnns	array	C	**Note:** This parameter is not applicable for QoS sustainability analytics.
dnais	array	C	**Note:** This parameter is not applicable for QoS sustainability analytics.
event	NwdafEvent	M	Indicates the subscribed event. The value for QoS sustainability analytics is "QOS Sustainability".

Table 9-34 (Cont.) EventSubscription

Parameter	Data Type	Presence	Description
extraReportReq	EventReportingRequirement	O	The additional event reporting requirements information.
ladnDnns	array	M	**Note:** This parameter is not applicable for QoS sustainability analytics.
loadLevelThreshold	Integer	C	**Note:** This parameter is not applicable for QoS sustainability analytics.
matchingDir	MatchingDirection	O	A matching direction can be provided along with a threshold. If this parameter is omitted, the default value is CROSSED.
nfLoadLvlThds	array	C	**Note:** This parameter is not applicable for QoS sustainability analytics.
visitedAreas	array	O	**Note:** This parameter is not applicable for QoS sustainability analytics.
maxTopAppUlNbr	Uinteger	O	**Note:** This parameter is not applicable for QoS sustainability analytics.
maxTopAppDlNbr	Uinteger	O	**Note:** This parameter is not applicable for QoS sustainability analytics.
nfInstanceIds	array	O	**Note:** This parameter is not applicable for QoS sustainability analytics.
nfSetIds	array	O	**Note:** This parameter is not applicable for QoS sustainability analytics.
nfTypes	array	O	**Note:** This parameter is not applicable for QoS sustainability analytics.
notificationMethod	NotificationMethod	O	Indicates the notification method.
nsiIdInfos	array	O	**Note:** This parameter is not applicable for QoS sustainability analytics.
nsiLevelThrds	array	O	**Note:** This parameter is not applicable for QoS sustainability analytics.
networkArea	NetworkAreaInfo	C	Identification of network area to which the subscription applies. The absence of this parameter implies the subscription is applicable for all network areas.

Table 9-34 (Cont.) EventSubscription

Parameter	Data Type	Presence	Description
qosRequ	QosRequirement	M	Indicates the QoS requirements when subscribed event is QOS_SUSTAINABILITY.
qosFlowRetThds	array	M	Represents the QoS flow retainability thresholds (provided by the consumer either for the 5QI or the GBR resource type specified in *qosRequ* parameter).
ranUeThrouThds	array	M	Represents the RAN UE throughput thresholds (provided by the consumer either for the 5QI or the non-GBR resource type specified in *qosRequ* parameter).
repetitionPeriod	DurationSec	C	This parameter is provided by the "notificationMethod" attribute if the notification method is "PERIODIC".
snssais	array	C	Identification(s) of network slice to which the subscription applies.
tgtUe	TargetUeInformation	O	Identifies target the UE information.
congThresholds	array	C	**Note:** This parameter is not applicable for QoS sustainability analytics.
nwPerfRequs	array	C	**Note:** This parameter is not applicable for QoS sustainability analytics.
bwRequs	array	O	**Note:** This parameter is not applicable for QoS sustainability analytics.
excepRequs	array	C	**Note:** This parameter is not applicable for QoS sustainability analytics.
exptAnaType	ExpectedAnalyticsType	C	**Note:** This parameter is not applicable for QoS sustainability analytics.
exptUeBehav	ExpectedUeBehaviourData	O	**Note:** This parameter is not applicable for QoS sustainability analytics.
ratFreqs	array	O	**Note:** This parameter is not applicable for QoS sustainability analytics.

Table 9-34 (Cont.) EventSubscription

Parameter	Data Type	Presence	Description
listOfAnaSubsets	array	O	**Note:** This parameter is not applicable for QoS sustainability analytics.
disperReqs	array	O	**Note:** This parameter is not applicable for QoS sustainability analytics.
redTransReqs	array	O	**Note:** This parameter is not applicable for QoS sustainability analytics.
wlanReqs	array	O	**Note:** This parameter is not applicable for QoS sustainability analytics.
upfInfo	UpfInformation	O	**Note:** This parameter is not applicable for QoS sustainability analytics.
appServerAddrs	array	C	**Note:** This parameter is not applicable for QoS sustainability analytics.
dnPerfReqs	array	O	**Note:** This parameter is not applicable for QoS sustainability analytics.

Table 9-35 QosRequirement

Parameter	Data Type	P	Cardinality	Description
5qi	5Qi	C	1	Represents a 5G QoS Identifier. It is included for standardized or preconfigured 5QIs.
gfbrUl	BitRate	C	0 to 1	Indicates Guaranteed Flow Bit Rate (GFBR) in the uplink. It is included for Guaranteed Bit Rate (GBR) 5QIs.
gfbrDl	BitRate	C	0 to 1	Indicates GFBR in the downlink. It is included for GBR 5QIs.
resType	QosResourceType	C	0 to 1	Resource type. It is provided for the nonstandardized and nonpreconfigured QoS characteristics.

Table 9-35 (Cont.) QosRequirement

Parameter	Data Type	P	Cardinality	Description
pdb	PacketDelBudget	O	0 to 1	Packet Delay Budget. This parameter may be provided for the non-standardized and non-pre-configured QoS characteristics.
per	PacketErrRate	O	0 to 1	Packet Error Rate. This parameter may be provided for the non-standardized and non-pre-configured QoS characteristics.
deviceSpeed	VelocityEstimate	O		The Velocity Estimate.
deviceType	DeviceType	O		The device type.

> **Note**
>
> Either 5QI within "5qi" attribute or the resource type within "resType" attribute is provided.

Table 9-36 5Qi

Type Name	Type Definition	Description
5Qi	Integer	Unsigned integer representing a 5G QoS Identifier (see, *3GPP TS 23.501 [8], subclause 5.7.2.1*). Range is 0 up to 255.

Table 9-37 PacketDelBudget

Type Name	Type Definition	Description
PacketDelBudget	Integer	Unsigned integer indicating Packet Delay Budget (see, *3GPP TS 23.501 [8], subclauses 5.7.3.4 and 5.7.4*). Expressed in milliseconds, minimum value = 1.

Table 9-38 PacketErrRate

Type Name	Type Definition	Description
PacketErrRate	Integer	Unsigned integer indicating Packet Error Rate (see, *3GPP TS 23.501 [8], subclauses 5.7.3.5 and 5.7.4*). Expressed in milliseconds, minimum value = 1..

Table 9-39 NnwdafEventsSubscriptionNotification

Parameter	Data Type	Presence	Description
eventNotifications	array	C	Notifications about individual events.
subscriptionId	String	M	String identifying a subscription to the Nnwdaf_EventsSubscription service.
notifCorrId	String	O	**Note:** This parameter is not applicable for QoS sustainability analytics.
oldSubscriptionId	String	C	**Note:** This parameter is not applicable for QoS sustainability analytics.
resourceUri	URI	C	**Note:** This parameter is not applicable for QoS sustainability analytics.
termCause	TermCause	O	**Note:** This parameter is not applicable for QoS sustainability analytics.

Table 9-40 EventNotification

Parameter	Data Type	Presence	Description
event	NwdafEvent	M	Subscribed events. The event parameter within event Subscriptions has to be "QOS _SUSTAINABILITY"
start	DateTime	O	It defines the start time from when the analytics information becomes valid.
expiry	DateTime	O	It defines the expiry time after which the analytics information is invalid.
timeStampGen	DateTime	C	It defines the timestamp of analytics generation.
failNotifyCode	NwdafFailureCode	C	**Note:** This parameter is not applicable for QoS sustainability analytics.

Table 9-40 (Cont.) EventNotification

Parameter	Data Type	Presence	Description
rvWaitTime	DurationSec	O	**Note:** This parameter is not applicable for QoS sustainability analytics.
anaMetaInfo	AnalyticsMetadataInfo	C	**Note:** This parameter is not applicable for QoS sustainability analytics.
nwPerfs	array	C	**Note:** This parameter is not applicable for QoS sustainability analytics.
nfLoadLevelInfos	array	C	**Note:** This parameter is not applicable for QoS sustainability analytics.
nsiLoadLevelInfos	array	C	**Note:** This parameter is not applicable for QoS sustainability analytics.
qosSustainInfos	array	C	The QOS sustainability information.
sliceLoadLevelInfo	SliceLoadLevelInformation	C	**Note:** This parameter is not applicable for QoS sustainability analytics.
svcExps	array		**Note:** This parameter is not applicable for QoS sustainability analytics.
ueComms	array	C	**Note:** This parameter is not applicable for QoS sustainability analytics.
ueMobs	array	C	**Note:** This parameter is not applicable for QoS sustainability analytics.
abnorBehavrs	array	C	**Note:** This parameter is not applicable for QoS sustainability analytics.
userDataCongInfos	array	C	**Note:** This parameter is not applicable for QoS sustainability analytics.
dnPerfInfos	array	C	**Note:** This parameter is not applicable for QoS sustainability analytics.
disperInfos	array	C	**Note:** This parameter is not applicable for QoS sustainability analytics.
redTransInfos	array	C	**Note:** This parameter is not applicable for QoS sustainability analytics.
wlanInfos	array	C	**Note:** This parameter is not applicable for QoS sustainability analytics.
smccExps	array	C	**Note:** This parameter is not applicable for QoS sustainability analytics.

Output QoS Sustainability Analytics

The following analytics information is obtained:

Table 9-41 Response Parameters

Parameter	Data Type	Presence	Description
event	NwdafEvent	M	Event that is notified.
start	DateTime	O	UTC time indicating the start time of the observation period. The absence of this attribute means subscription at present time.
expiry	DateTime	O	It defines the expiration time after which the analytics information becomes invalid.
timeStampGen	DateTime	C	It defines the timestamp of analytics generation.
QosSustainabilityInfo	QosSustainabilityInfo	C	The QoS sustainability analytics information.

QosSustainabilityInfo

Table 9-42 QosSustainabilityInfo

Attribute Name	Data Type	P	Cardinality	Description
areaInfo	NetworkAreaInfo	M	1	The network area information.
startTs	DateTime	M	1	UTC time indicating the start time of the observation period.
endTs	DateTime	M	1	UTC time indicating the end time of the observation period.
qosFlowRetThd	RetainabilityThreshold	O	0 to 1	The reporting QoS Flow Retainability Threshold that is met or crossed for 5QI of GBR resource type.
ranUeThrouThd	BitRate	O	0 to 1	The reporting RAN UE Throughput Threshold that is met or crossed for 5QI of non-GBR resource type.

Table 9-42 (Cont.) QosSustainabilityInfo

Attribute Name	Data Type	P	Cardinality	Description
snssai	Snssai	C	0 to 1	Identifies an S-NSSAI. Is present if the "snssais" was provided within the EventSubscription during the subscription for event notification procedure.
5qi	Integer	M	1	The subscribed 5qi type.
confidence	Uinteger	C	0 to 1	Indicates the confidence of the prediction. If sufficient data is unavailable during the specified analytics target time interval, the confidence value returned is "0". This attribute is present in analytics prediction.

> **Note**
>
> Either of the attributes *qosFlowRetThd* or *ranUeThrouThd* are provided.

> **Note**
>
> If the requested observation period identified by the "startTs" and "endTs" attributes in the "EventReportingRequirement" type is a future time interval, it implies that the analytics result is a prediction.

NetworkAreaInfo

Table 9-43 NetworkAreaInfo

Attribute name	Data type	P	Cardinality	Description
ecgis	array	O	0 to N	Is the list of E-UTRA cell identities.
ncgis	array	O	0 to N	Is the list of NR cell identities

Table 9-43 (Cont.) NetworkAreaInfo

Attribute name	Data type	P	Cardinality	Description
gRanNodeIds	array	O	0 to N	Is the list of list of the NG-RAN nodes.
tais	array	O	0 to N	Is the list of tracking area identities.

RetainabilityThreshold

Table 9-44 RetainabilityThreshold

Attribute Name	Data type	P	Cardinality	Description
relFlowNum	Uinteger	O	0 to 1	The number of abnormally released QoS flows.
relTimeUnit	TimeUnit	C	0 to 1	The time unit of the active session, present if *relFlowNum* is present.
relFlowRatio	SamplingRatio	O	0 to 1	Ratio of abnormally released QoS flows to the total released QoS flows, expressed as a percentage.

> **Note**
>
> Either *relFlowNum* and its associated *relTimeUnit* or *relFlowRatio* are provided. The *relFlowNum* and *relTimeUnit* together represents the number of abnormally released QoS flows (that is, *relFlowNum*) within the time unit (that is, *relTimeUnit*).

BitRate

Table 9-45 BitRate

Type Name	Type Definition	Description
BitRate	String	String representing a bit rate that is formatted as follows: *Pattern: '^\d+(\.\d+)? (bps|Kbps|Mbps|Gbps|Tbps)$'* For example: "125 Mbps", "0.125 Gbps", "125000 Kbps"

Create a QoS Sustainability Analytics Subscription

This service operation is used to create a QoS sustainability analytics subscription.

Type: POST

URI:`{apiroot}:{serverPort}:/nnwdaf-eventsubscription/<api version>/subscriptions`

Initiated By: Consumers

Table 9-46 Endpoint Parameters

Parameter	Description	Example
`{apiroot}`	The IP used to access the OCNWDAF subscription.	
`{serverport}`	The port used to access the OCNWDAF subscription. Default value is 8080.	
`{subscriptionId}`	Subscription ID	
`{analyticsId}`	The analytics ID is "QOS_SUSTAINABILITY"	
`{supported-features}`	100	
`{tgt-ue}`	Encoded Target UE information.	`{ "supis": null, "intGroupIds": null, "anyUe": true }`

Table 9-46 (Cont.) Endpoint Parameters

Parameter	Description	Example

{event-filter}	Encoded event filter value.	<pre>{
		"anySlice": false,
		"snssais": [
		{
		"sst": "2",
		"sd":
		"405060"
		}
		],
		"networkArea": {
		"ecgis": [
		{
		
		"plmnId": {
		
		"mcc": "611",
		
		"mnc": "946"
		},
		
		"eutraCellId":
		"60De3B8",
		"nid":
		"2f9CcfeEC9a"
		}
		],
		"ncgis": [
		{
		
		"plmnId": {
		
		"mcc": "375",
		
		"mnc": "36"
		},
		
		"nrCellId": "07A78F009",
		"nid":
		"e5D8B1EbD11"
		}
		],
		"gRanNodeIds": [
		{
		
		"plmnId": {
		
		"mcc": "791",
		
		"mnc": "230"</pre>

Table 9-46 (Cont.) Endpoint Parameters

Parameter	Description	Example

		},
		"n3IwfId": "CB1E5ba",
		"gNbId": {
		"bitLength": 32,
		"gNBValue": "BF6B9E"
		},
		"ngeNbId": "SMacroNGeNB-F5CCC",
		"wagfId": "8f",
		"tngfId": "1a473d3D",
		"nid": "BFbBAabEBD3",
		"eNbId": "MacroeNB-f26ab"
		}
		],
		"tais": [
		{
		"plmnId": {
		"mcc": "585",
		"mnc": "162"
		},
		"tac": "ebef4B",
		"nid": "fDfC6bbC673"
		}
		]
		},
		"qosRequ": {
		"5qi": 1
		},
		"nwPerfTypes": [
		"NUM_OF_UE"
		]
		}

Table 9-46 (Cont.) Endpoint Parameters

Parameter	Description	Example

{ana-req}	Encoded value of analytics requirements.	{
		
		"startTs":"2023-02-08T12:00:10.000021",
		
		"endTs":"2023-05-13T12:02:05.000000",
		
		"timeAnaNeeded":"2024-12-13T12:00:01.000000",
		
		"maxObjectNbr":10,
		
		"sampRatio":1
		
		}

Table 9-47 Supported Response Codes

Code	Description
201	The subscription is created successfully.
400	Bad Request. The request is incorrect and subscription is not created.
500	Indicates a internal server processing error.

Examples

The following example shows how an NF creates a subscription for QoS sustainability analytics by submitting a POST request on the REST resource using cURL.

cURL Command

```
curl --location '10.123.159.23:8087/nnwdaf-eventssubscription/v1/
subscriptions' \
--header 'accept: application/json' \
--header 'Content-Type: application/json' \
--data '{
    "notificationURI": "http://prodcon-1:9282/receive",
    "supportedFeatures": "008",
    "eventSubscriptions": [
        {
            "event": "QOS_SUSTAINABILITY",
            "networkArea": {
                "ecgis": [
```

```
                {
                    "plmnId": {
                        "mcc": "611",
                        "mnc": "946"
                    },
                    "eutraCellId": "60De3B8",
                    "nid": "2f9CcfeEC9a"
                }
            ],
            "ncgis": [
                {
                    "plmnId": {
                        "mcc": "375",
                        "mnc": "36"
                    },
                    "nrCellId": "eFdEDcE7D",
                    "nid": "e5D8B1EbD11"
                }
            ],
            "gRanNodeIds": [
                {
                    "plmnId": {
                        "mcc": "791",
                        "mnc": "230"
                    },
                    "n3IwfId": "CB1E5ba",
                    "gNbId": {
                        "bitLength": 32,
                        "gNBValue": "BF6B9E"
                    },
                    "ngeNbId": "SMacroNGeNB-F5CCC",
                    "wagfId": "8f",
                    "tngfId": "1a473d3D",
                    "nid": "BFbBAabEBD3",
                    "eNbId": "MacroeNB-f26ab"
                }
            ],
            "tais": [
                {
                    "plmnId": {
                        "mcc": "585",
                        "mnc": "162"
                    },
                    "tac": "ebef4B",
                    "nid": "fDfC6bbC673"
                }
            ]
        },
        "extraReportReq": {
            "startTs": "2020-07-08T00:00:00.000Z",
            "endTs": "2023-12-21T18:59:40.694Z"
        },
        "notificationMethod": "THRESHOLD",
        "matchingDir": "CROSSED",
        "qosRequ": {
            "5qi": 1,
```

```
                    "resType": "NON_GBR/NON_CRITICAL_GBR/CRITICAL_GBR"
                },
                "qosFlowRetThds": [
                    {
                        "relTimeUnit": "MINUTE/HOUR/DAY"
                    }
                ],
                "repetitionPeriod": 0,
                "snssais": [
                    {
                        "sst": 1,
                        "sd": "102030"
                    }
                ],
                "tgtUe": {
                    "anyUe": true
                }
            }
        ],
        "evtReq": {
            "immRep": false,
            "notifMethod": "ON_EVENT_DETECTION",
            "maxReportNbr": 50,
            "monDur": "2023-12-21T18:59:40.694Z",
            "repPeriod": 0,
            "sampRatio": 75,
            "grpRepTime": 0
        },
        "notificationURI": "http://10.123.159.82:31456/receive",
        "supportedFeatures": "008"
}
```

Example of the Request Body

```
{
    "notificationURI": "http://prodcon-1:9282/receive",
    "supportedFeatures": "008",
    "eventSubscriptions": [
        {
            "event": "QOS_SUSTAINABILITY",
            "networkArea": {
                "ecgis": [
                    {
                        "plmnId": {
                            "mcc": "611",
                            "mnc": "946"
                        },
                        "eutraCellId": "60De3B8",
                        "nid": "2f9CcfeEC9a"
                    }
                ],
                "ncgis": [
                    {
                        "plmnId": {
                            "mcc": "375",
```

```
                    "mnc": "36"
                },
                "nrCellId": "eFdEDcE7D",
                "nid": "e5D8B1EbD11"
            }
        ],
        "gRanNodeIds": [
            {
                "plmnId": {
                    "mcc": "791",
                    "mnc": "230"
                },
                "n3IwfId": "CB1E5ba",
                "gNbId": {
                    "bitLength": 32,
                    "gNBValue": "BF6B9E"
                },
                "ngeNbId": "SMacroNGeNB-F5CCC",
                "wagfId": "8f",
                "tngfId": "1a473d3D",
                "nid": "BFbBAabEBD3",
                "eNbId": "MacroeNB-f26ab"
            }
        ],
        "tais": [
            {
                "plmnId": {
                    "mcc": "585",
                    "mnc": "162"
                },
                "tac": "ebef4B",
                "nid": "fDfC6bbC673"
            }
        ]
    },
    "extraReportReq": {
        "startTs": "2020-07-08T00:00:00.000Z",
        "endTs": "2023-12-21T18:59:40.694Z"
    },
    "notificationMethod": "THRESHOLD",
    "matchingDir": "CROSSED",
    "qosRequ": {
        "5qi": 1,
        "resType": "NON_GBR/NON_CRITICAL_GBR/CRITICAL_GBR"
    },
    "qosFlowRetThds": [
        {
            "relTimeUnit": "MINUTE/HOUR/DAY"
        }
    ],
    "repetitionPeriod": 0,
    "snssais": [
        {
            "sst": 1,
            "sd": "102030"
        }
```

```
            ],
            "tgtUe": {
                "anyUe": true
            }
        }
    ],
    "evtReq": {
        "immRep": false,
        "notifMethod": "ON_EVENT_DETECTION",
        "maxReportNbr": 50,
        "monDur": "2023-12-21T18:59:40.694Z",
        "repPeriod": 0,
        "sampRatio": 75,
        "grpRepTime": 0
    },
    "notificationURI": "http://10.123.159.82:31456/receive",
    "supportedFeatures": "008"
}
```

Example of the Response Body

```
{
    "eventSubscriptions": [
        {
            "event": "QOS_SUSTAINABILITY",
            "networkArea": {
                "ecgis": [
                    {
                        "plmnId": {
                            "mcc": "611",
                            "mnc": "946"
                        },
                        "eutraCellId": "60De3B8",
                        "nid": "2f9CcfeEC9a"
                    }
                ],
                "ncgis": [
                    {
                        "plmnId": {
                            "mcc": "375",
                            "mnc": "36"
                        },
                        "nrCellId": "eFdEDcE7D",
                        "nid": "e5D8B1EbD11"
                    }
                ],
                "gRanNodeIds": [
                    {
                        "plmnId": {
                            "mcc": "791",
                            "mnc": "230"
                        },
                        "n3IwfId": "CB1E5ba",
                        "gNbId": {
                            "bitLength": 32,
```

```
                            "gNBValue": "BF6B9E"
                        },
                        "ngeNbId": "SMacroNGeNB-F5CCC",
                        "wagfId": "8f",
                        "tngfId": "1a473d3D",
                        "nid": "BFbBAabEBD3",
                        "eNbId": "MacroeNB-f26ab"
                    }
                ],
                "tais": [
                    {
                        "plmnId": {
                            "mcc": "585",
                            "mnc": "162"
                        },
                        "tac": "ebef4B",
                        "nid": "fDfC6bbC673"
                    }
                ]
            },
            "extraReportReq": {
                "startTs": "2020-07-08T00:00:00.000Z",
                "endTs": "2023-12-21T18:59:40.694Z"
            },
            "notificationMethod": "THRESHOLD",
            "matchingDir": "CROSSED",
            "qosRequ": {
                "5qi": 1,
                "resType": "NON_GBR/NON_CRITICAL_GBR/CRITICAL_GBR"
            },
            "qosFlowRetThds": [
                {
                    "relTimeUnit": "MINUTE/HOUR/DAY"
                }
            ],
            "repetitionPeriod": 0,
            "snssais": [
                {
                    "sst": 1,
                    "sd": "102030"
                }
            ],
            "tgtUe": {
                "anyUe": true
            }
        }
    ],
    "evtReq": {
        "immRep": false,
        "notifMethod": "ON_EVENT_DETECTION",
        "maxReportNbr": 50,
        "monDur": "2023-12-21T18:59:40.694Z",
        "repPeriod": 0,
        "sampRatio": 75,
        "grpRepTime": 0
    },
```

```
    "notificationURI": "http://10.123.159.82:31456/receive",
    "supportedFeatures": "008"
}
}
```

Modify an Existing QoS Sustainability Analytics Subscription

This service operation is used to modify an existing QoS sustainability Analytics subscription.

Type: PUT

URI: `{apiroot}:{serverPort}:/nnwdaf-eventsubscription/<api version>/subscriptions/{subscriptionId}`

For information on endpoint parameters see, Table 9-46.

Initiated By: Consumers

For information on request body parameters see, Table 9-33

Table 9-48 Supported Response Codes

Code	Description
204	The subscription resource is successfully updated.
400	Bad Request The request is incorrect and subscription is not updated.
500	Indicates a internal server processing error.

Examples

The following example shows how an NF updates a QoS sustainability Analytics subscription by submitting a PUT request on the REST resource using cURL.

cURL Command

```
curl --location --request PUT '10.123.159.23:8087/nnwdaf-
eventssubscription/v1/subscriptions/371d8527-dcc9-4179-9d67-82e5c93fc206' \
--header 'Content-Type: application/json' \
--data '
{
    "notificationURI": "http://prodcon-1:9282/receive",
    "supportedFeatures": "008",
    "eventSubscriptions": [
        {
            "event": "QOS_SUSTAINABILITY",
            "networkArea": {
                "ecgis": [
                    {
                        "plmnId": {
                            "mcc": "611",
                            "mnc": "946"
                        },
                        "eutraCellId": "60De3B8",
                        "nid": "2f9CcfeEC9a"
                    }
                ],
```

```
        "ncgis": [
            {
                "plmnId": {
                    "mcc": "375",
                    "mnc": "36"
                },
                "nrCellId": "eFdEDcE7D",
                "nid": "e5D8B1EbD11"
            }
        ],
        "gRanNodeIds": [
            {
                "plmnId": {
                    "mcc": "791",
                    "mnc": "230"
                },
                "n3IwfId": "CB1E5ba",
                "gNbId": {
                    "bitLength": 32,
                    "gNBValue": "BF6B9E"
                },
                "ngeNbId": "SMacroNGeNB-F5CCC",
                "wagfId": "8f",
                "tngfId": "1a473d3D",
                "nid": "BFbBAabEBD3",
                "eNbId": "MacroeNB-f26ab"
            }
        ],
        "tais": [
            {
                "plmnId": {
                    "mcc": "585",
                    "mnc": "162"
                },
                "tac": "ebef4B",
                "nid": "fDfC6bbC673"
            }
        ]
    },
    "extraReportReq": {
        "startTs": "2020-07-08T00:00:00.000Z",
        "endTs": "2023-12-21T18:59:40.694Z"
    },
    "notificationMethod": "THRESHOLD",
    "matchingDir": "CROSSED",
    "qosRequ": {
        "5qi": 1,
        "resType": "NON_GBR/NON_CRITICAL_GBR/CRITICAL_GBR"
    },
    "qosFlowRetThds": [
        {
            "relTimeUnit": "MINUTE/HOUR/DAY"
        }
    ],
    "repetitionPeriod": 0,
    "snssais": [
```

```
                {
                    "sst": 1,
                    "sd": "102030"
                }
            ],
            "tgtUe": {
                "anyUe": true
            }
        }
    ],
    "evtReq": {
        "immRep": false,
        "notifMethod": "ON_EVENT_DETECTION",
        "maxReportNbr": 50,
        "monDur": "2023-12-21T18:59:40.694Z",
        "repPeriod": 0,
        "sampRatio": 75,
        "grpRepTime": 0
    },
    "notificationURI": "http://10.123.159.82:31456/receive",
    "supportedFeatures": "008"
}
```

Example of the Request Body

```
{
    "notificationURI": "http://prodcon-1:9282/receive",
    "supportedFeatures": "008",
    "eventSubscriptions": [
        {
            "event": "QOS_SUSTAINABILITY",
            "networkArea": {
                "ecgis": [
                    {
                        "plmnId": {
                            "mcc": "611",
                            "mnc": "946"
                        },
                        "eutraCellId": "60De3B8",
                        "nid": "2f9CcfeEC9a"
                    }
                ],
                "ncgis": [
                    {
                        "plmnId": {
                            "mcc": "375",
                            "mnc": "36"
                        },
                        "nrCellId": "eFdEDcE7D",
                        "nid": "e5D8B1EbD11"
                    }
                ],
                "gRanNodeIds": [
                    {
                        "plmnId": {
```

```
                            "mcc": "791",
                            "mnc": "230"
                        },
                        "n3IwfId": "CB1E5ba",
                        "gNbId": {
                            "bitLength": 32,
                            "gNBValue": "BF6B9E"
                        },
                        "ngeNbId": "SMacroNGeNB-F5CCC",
                        "wagfId": "8f",
                        "tngfId": "1a473d3D",
                        "nid": "BFbBAabEBD3",
                        "eNbId": "MacroeNB-f26ab"
                    }
                ],
                "tais": [
                    {
                        "plmnId": {
                            "mcc": "585",
                            "mnc": "162"
                        },
                        "tac": "ebef4B",
                        "nid": "fDfC6bbC673"
                    }
                ]
            },
            "extraReportReq": {
                "startTs": "2020-07-08T00:00:00.000Z",
                "endTs": "2023-12-21T18:59:40.694Z"
            },
            "notificationMethod": "THRESHOLD",
            "matchingDir": "CROSSED",
            "qosRequ": {
                "5qi": 1,
                "resType": "NON_GBR/NON_CRITICAL_GBR/CRITICAL_GBR"
            },
            "qosFlowRetThds": [
                {
                    "relTimeUnit": "MINUTE/HOUR/DAY"
                }
            ],
            "repetitionPeriod": 0,
            "snssais": [
                {
                    "sst": 1,
                    "sd": "102030"
                }
            ],
            "tgtUe": {
                "anyUe": true
            }
        }
    ],
    "evtReq": {
        "immRep": false,
        "notifMethod": "ON_EVENT_DETECTION",
```

```
        "maxReportNbr": 50,
        "monDur": "2023-12-21T18:59:40.694Z",
        "repPeriod": 0,
        "sampRatio": 75,
        "grpRepTime": 0
    },
    "notificationURI": "http://10.123.159.82:31456/receive",
    "supportedFeatures": "008"
}
```

Obtain QoS Sustainability Analytics Subscription Information

This service operation is used to obtain information about an existing QoS Analytics subscription.

Type: GET

URI: `{apiroot}:{serverPort}:/nnwdaf-eventsubscription/<api version>/subscriptions/{subscriptionId}?event-id={analyticsId}&supported-features={supported-features}&tgt-ue={tgt-ue}&event-filter={event-filter}&ana-req={ana-req}`

For information on endpoint parameters see, Table 9-46.

Initiated By: Consumers

For information on request body parameters see, Table 9-33.

Examples

The following example shows how an NF gets subscription information by submitting a GET request on the REST resource using cURL.

cURL Command

```
curl --location 'http://10.123.159.29:8080/nnwdaf-analyticsinfo/v1/analytics?event-id=QOS_SUSTAINABILITY&supported-features=008&tgt-ue=%257B%250A%2520%2520%2520%2520%2520%2520%2520%2520%2522supis%2522%253A%2520null%252C%250A%2520%2520%2520%2520%2520%2520%2520%2520%2522intGroupIds%2522%253A%2520null%252C%250A%2520%2520%2520%2520%2520%2520%2520%2520%2522anyUe%2522%253A%2520true%250A%257D&event-filter=%257B%2522anySlice%2522%253Afalse%252C%2522appIds%2522%253A%255B%2522IQPKITNJSE%2522%255D%252C%2522dnns%2522%253A%255B%2522KCRFf30.lafQu2.fOntr02%2522%255D%252C%2522dnais%2522%253A%255B%2522KuDMa.fDOC%2540DgvaY7.dQUxS69.uTvFz6KCRFf30.lafQu2.fOntr02%2522%255D%252C%2522networkArea%2522%253A%257B%2522ecgis%2522%253A%255B%257B%2522plmnId%2522%253A%257B%2522mcc%2522%253A%2522611%2522%252C%2522mnc%2522%253A%2522946%2522%257D%252C%2522eutraCellId%2522%253A%252260De3B8%2522%252C%2522nid%2522%253A%25222f9CcfeEC9a%2522%257D%255D%252C%2522ncgis%2522%253A%255B%257B%2522plmnId%2522%253A%257B%2522mcc%2522%253A%2522375%2522%252C%2522mnc%2522%253A%252236%2522%257D%252C%2522nrCellId%2522%253A%2522eFdEDcE7D%2522%252C%2522nid%2522%253A%2522e5D8B1EbD11%2522%257D%255D%252C%2522plmnId%2522%253A%257B%2522mcc%2522%253A%2522791%2522%252C%2522mnc%2522%253A%2522230%2522%257D%252C%2522n3IwfId%2522%253A%2522CB1E5ba%2522%252C%2522gNbId%2522%253A%257B%2522bitLength%2522%253A32%252C%2522gNBValue%2522%253A%2522BF6B9E%2522%257D%252C%2522ngeNbId%2522%253A%2522SMacroNGeNB-F5CCC%2522%252C%2522wagfId%2522%253A%25228f%2522%252C%2522tngfId%2522%253A%2521a473d3D%2522%252C%2522nid%2522%253A%2522BFbBAabEBD3%2522%252C%2522eNbId%2522%253A%2522MacroeNB-
```

```
f26ab%2522%257D%255D%252C%2522tais%2522%253A%255B%257B%2522plmnId%2522%253A%25
7B%2522mcc%2522%253A%2522585%2522%252C%2522mnc%2522%253A%2522162%2522%257D%252
C%2522tac%2522%253A%2522ebef4B%2522%252C%2522nid%2522%253A%2522fDfC6bbC673%252
2%257D%255D%257D%252C%2522nwPerfTypes%2522%253A%255B%2522NUM_OF_UE%2522%255D%2
57D&ana-
req=%257B%250A%2520%2520%2520%2520%2522startTs%2522%253A%25222020-07-08T12%253
A00%253A10.000021%2522%252C%250A%2520%2520%2520%2520%2522endTs%2522%253A%25222
021-12-13T12%253A02%253A05.000000%2522%252C%250A%2520%2520%2520%2520%2522timeA
naNeeded%2522%253A%25222022-12-13T12%253A00%253A01.000000%2522%252C%250A%2520%
2520%2520%2520%2522maxObjectNbr%2522%253A0%252C%250A%2520%2520%2520%2520%2522s
ampRatio%2522%253A1%250A%257D'
```

Example of the Response Body

```
{
    "eventSubscriptions": [
        {
            "event": "QOS_SUSTAINABILITY",
            "networkArea": {
                "ecgis": [
                    {
                        "plmnId": {
                            "mcc": "611",
                            "mnc": "946"
                        },
                        "eutraCellId": "60De3B8",
                        "nid": "2f9CcfeEC9a"
                    }
                ],
                "ncgis": [
                    {
                        "plmnId": {
                            "mcc": "375",
                            "mnc": "36"
                        },
                        "nrCellId": "eFdEDcE7D",
                        "nid": "e5D8B1EbD11"
                    }
                ],
                "gRanNodeIds": [
                    {
                        "plmnId": {
                            "mcc": "791",
                            "mnc": "230"
                        },
                        "n3IwfId": "CB1E5ba",
                        "gNbId": {
                            "bitLength": 32,
                            "gNBValue": "BF6B9E"
                        },
                        "ngeNbId": "SMacroNGeNB-F5CCC",
                        "wagfId": "8f",
                        "tngfId": "1a473d3D",
                        "nid": "BFbBAabEBD3",
                        "eNbId": "MacroeNB-f26ab"
```

```
                        }
                    ],
                    "tais": [
                        {
                            "plmnId": {
                                "mcc": "585",
                                "mnc": "162"
                            },
                            "tac": "ebef4B",
                            "nid": "fDfC6bbC673"
                        }
                    ]
                },
                "extraReportReq": {
                    "startTs": "2020-07-08T00:00:00.000Z",
                    "endTs": "2023-12-21T18:59:40.694Z"
                },
                "notificationMethod": "THRESHOLD",
                "matchingDir": "CROSSED",
                "qosRequ": {
                    "5qi": 1,
                    "resType": "NON_GBR/NON_CRITICAL_GBR/CRITICAL_GBR"
                },
                "qosFlowRetThds": [
                    {
                        "relTimeUnit": "MINUTE/HOUR/DAY"
                    }
                ],
                "repetitionPeriod": 0,
                "snssais": [
                    {
                        "sst": 1,
                        "sd": "102030"
                    }
                ],
                "tgtUe": {
                    "anyUe": true
                }
            }
        ],
        "evtReq": {
            "immRep": false,
            "notifMethod": "ON_EVENT_DETECTION",
            "maxReportNbr": 50,
            "monDur": "2023-12-21T18:59:40.694Z",
            "repPeriod": 0,
            "sampRatio": 75,
            "grpRepTime": 0
        },
        "notificationURI": "http://10.123.159.82:31456/receive",
        "supportedFeatures": "008"
    }
```


Delete an Existing QoS Sustainability Analytics Subscription

This service operation is used to delete an existing QoS sustainability analytics subscription.

Type: DELETE

URI: `{apiroot}:{serverPort}:/nnwdaf-eventsubscription/<api version>/subscriptions/{subscriptionId}`

For information on endpoint parameters see, Table 9-46.

Initiated By: Consumers

Table 9-49 Supported Response Codes

Code	Description
204	The subscription resource is successfully deleted.
404	Not found

The following example shows how an NF deletes subscription information by submitting a DELETE request on the REST resource using cURL.

cURL Command

```
curl --location '10.123.159.23:8087/nnwdaf-eventssubscription/v1/subscriptions/371d8527-dcc9-4179-9d67-82e5c93fc206'
```

10
OCNWDAF Alerts

This chapter describes the following information about OCNWDAF alerts and KPIs:

- OCNWDAF Alert Configuration
  - System Level Alerts
  - Application Level Alerts
- SNMP Support
- OCNWDAF KPIs

10.1 OCNWDAF Alert Configuration

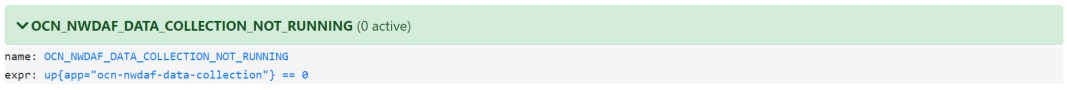
This section describes the measurement based alert rules configuration for OCNWDAF. The Alert Manager uses the Prometheus measurements values as reported by microservices in conditions under alert rules to trigger alerts.

OCNWDAF Alert configuration in Prometheus

The following procedure is used to configure alerts in Prometheus:

1. Download the `ocn-nwdaf-alerting-rules.yaml` file. Edit this file to configure the alert rules. The parameters in the file that can be edited include `name` of the alert, `rules` for the alert including `alert` name and the expression `expr` defined to trigger the alert.
2. Copy the updated `ocn-nwdaf-alerting-rules.yaml` file to Bastion Host.
3. Run the following command:
   ```
   kubectl apply -f ocn-nwdaf-alerting-rules.yaml -n ocn-nwdaf
   ```
4. To verify if the Custom Resource Definition (CRD) is created, run the following command:
   ```
   kubectl get prometheusrule -n ocn-nwdaf
   ```
5. Verify the alerts in the Prometheus GUI, the alert name and expression is listed. See example below:

Figure 10-1 Prometheus GUI



Alert Rules

The alerts are configured on the Prometheus server. The metrics scraped correspond to a pod that runs a single microservice, so each alert belongs to one of the pods running. Prometheus continously collects metrics and when any of the alerting rules are met, the alert is triggered. All the alert rules are written in one or multiple `.yml` files and deployed as described in procedure OCNWDAF Alert configuration in Prometheus. Listed below are the alert rules for the various alerts captured for OCNWDAF:

Status Alert Rule

```
- name: <ALERT NAME>
    rules:
    - alert: <ALERT NAME>
      expr: up{app="SERVICE LABEL"} == 0
```

Example:

```
 - name: OCN_NWDAF_DATA_COLLECTION_NOT_RUNNING
    rules:
    - alert: OCN_NWDAF_DATA_COLLECTION_NOT_RUNNING
      expr: up{app="ocn-nwdaf-data-collection"} == 0
```

Traffic Alert Rule

- Request rate rule:

  ```
  - name: <ALERT NAME>
      rules:
      - alert: <ALERT NAME>
        expr: >
        sum
  without(method,status,outcome,exception,app,instance,container,pod,pod_temp
  late_hash) (rate(http_server_requests_seconds_count{uri="<URI ENDPOINT>"}
  [1m])) > 1000
  ```

  Example:

  ```
    - name: HIGH_ABNORMAL_BEHAVIOUR_REQUEST_RATE
      rules:
      - alert: HIGH_ABNORMAL_BEHAVIOUR_REQUEST_RATE
        expr: sum
  without(method,status,outcome,exception,app,instance,container,pod,pod_temp
  late_hash) (rate(http_server_requests_seconds_count{uri="nnwdaf-
  analyticsinfo/v1/analytics?event-id=ABNORMAL_BEHAVIOUR"}[1m])) > 1000
  ```

- Failure rate request rule:

  ```
  - name: <ALERT NAME>
      rules:
      - alert: <ALERT NAME>
        expr: >
       (sum
  without(method,outcome,exception,app,instance,container,pod,pod_template_ha
  sh) (rate(http_server_requests_seconds_count{uri="<URI
  ENDPOINT>",status=~"[4-5].."}[1m]))/ ignoring(status) sum
  without(method,status,outcome,exception,app,instance,container,pod,pod_temp
  late_hash) (rate(http_server_requests_seconds_count{uri="<URI ENDPOINT>"}
  [1m]))) * 100 > 70
  ```

Example:

```
 - name: HIGH_ABNORMAL_BEHAVIOUR_REQUEST_FAILURE_RATE
    rules:
    - alert: HIGH_ABNORMAL_BEHAVIOUR_REQUEST_FAILURE_RATE
      expr: (sum
without(method,outcome,exception,app,instance,container,pod,pod_template_ha
sh) (rate(http_server_requests_seconds_count{uri="nnwdaf-analyticsinfo/v1/
analytics?event-id=ABNORMAL_BEHAVIOUR",status=~"[4-5].."}[1m]))/
ignoring(status) sum
without(method,status,outcome,exception,app,instance,container,pod,pod_temp
late_hash) (rate(http_server_requests_seconds_count{uri="nnwdaf-
analyticsinfo/v1/analytics?event-id=ABNORMAL_BEHAVIOUR"}[1m]))) * 100 > 70
```

CPU Alert Rule

```
- name: <ALERT NAME>
    rules:
    - alert: <ALERT NAME>
      expr: system_cpu_usage{app="<SERVICE LABEL>"} * 100 > 80
```

Example:

```
 - name: OCN_NWDAF_DATA_COLLECTION_HIGH_CPU_LOAD
    rules:
    - alert: OCN_NWDAF_DATA_COLLECTION_HIGH_CPU_LOAD
      expr: system_cpu_usage{app="ocn-nwdaf-data-collection"} * 100 > 80
```

JVM Memory Usage Alert Rule

```
 - name: <ALERT NAME>
    rules:
    - alert: <ALERT NAME>
      expr: >

      (sum(avg_over_time(jvm_memory_used_bytes{area="heap",app="<SERVICE
LABEL>"} [1m]))/
sum(avg_over_time(jvm_memory_max_bytes{area="heap",app="<SERVICE LABEL>"}
[1m]))) * 100 > 80
```

Example:

```
 - name: OCN_NWDAF_DATA_COLLECTION_HIGH_JVM_HEAP_MEMORY_USAGE
    rules:
    - alert: OCN_NWDAF_DATA_COLLECTION_HIGH_JVM_HEAP_MEMORY_USAGE
      expr: (sum(avg_over_time(jvm_memory_used_bytes{area="heap",app="ocn-
nwdaf-data-collection"} [1m]))/
sum(avg_over_time(jvm_memory_max_bytes{area="heap",app="ocn-nwdaf-data-
collection"}[1m]))) * 100 > 80
```

10.1.1 SNMP Support

Simple Network Management Protocol (SNMP) is an application-layer protocol designed for monitoring and managing network devices within a Local Area Network (LAN) or Wide Area Network (WAN).

OCNWDAF forwards the Prometheus alerts as Simple Network Management Protocol (SNMP) traps to the southbound SNMP servers. OCNWDAF uses two SNMP MIB files to generate the traps. Update the *alertmanager.yaml* file to configure the alert manager. In the *alertmanager.yaml* file, the alerts can be grouped based on podname, alertname, severity, namespace, and so on. The Prometheus Alert Manager is integrated with 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 and alert manager files to fetch the SNMP traps in their environment.

Configuring SNMP Support

The *alertmanager.yaml* file is updated to include additional information for SNMP traps.

Sample of the *alertmanager.yaml* file:

```
{{- range $key, $svcName := .Values.global.rules.services }}
- alert: {{ $svcName | replace "-" "_" | upper }}_HIGH_CPU_LOAD
  expr: system_cpu_usage{job={{ $svcName | quote }},
namespace={{ $.Release.Namespace | quote }} } * 100 > 90
  for: 5m
  labels:
    alertname: "OCN_NWDAF_SVC_HIGH_CPU_LOAD"
    oid: "1.3.6.1.4.1.323.5.3.45.1.
{{ index $.Values.global.rules.oid $svcName }}.4002"
    severity: critical
    namespace: {{ $.Release.Namespace | quote }}
  annotations:
    namespace: {{ $.Release.Namespace | quote }}
    severity: critical
    summary: "Service {{ "{{$labels.app}}" }} CPU load is high."
    description: "Service {{ "{{$labels.app}}" }} CPU load has been high for
more than 5 minutes."
{{- end }}
```

Configure the SNMP Test Client

Follow the steps below to configure the SNMP Test Client:

1. Create a *ConfigMap* that includes the MIB files. Run the following command:

   ```
   kubectl create configmap my-config --from-file=/path/to/mib/files/ -n
   <namespace>
   ```

   Where, `my-config` is the name of the *ConfigMap*. The same has to be used in the pod configuration file. The *ConfigMap* must be in the same namespace where the SNMP client is deployed.

2. To start the SNMP trap daemon service, use the service configuration *.yaml* file, see the example below:

```
apiVersion: v1
kind: Service
metadata:
  labels:
    name: snmptrapd
  name: snmptrapd
  namespace: performance-idc  // namespace in which you want to deploy the
service
spec:
  ports:
  - name: snmptrapd
    port: 162
    protocol: UDP
    targetPort: 162
  selector:
    name: snmptrapd
  sessionAffinity: None
  type: ClusterIP
```

3. Use the following pod deployment configuration to deploy the pod corresponding to the above service. The commands mentioned in this file add the MIB files from the *ConfigMap* to the pod, following which the SNMP trap daemon service application starts.
Sample docker file:

```
FROM ocr-docker-remote.artifactory.oci.oraclecorp.com/os/oraclelinux:8-slim
ARG HTTPS_PROXY=http://www-proxy.us.oracle.com:80
RUN echo -e "[main]\nproxy=${HTTPS_PROXY}" >> /etc/dnf/dnf.conf
RUN microdnf update -y && microdnf install -y lsof
RUN microdnf install net-snmp
ADD snmptrapd.conf /etc/snmp/snmptrapd.conf
EXPOSE 162
CMD ["/bin/sh"]
```

Sample *snmp-pod.yaml* file:

```
apiVersion: v1
kind: Pod
metadata:
  name: snmptrapd
  labels:
    name: snmptrapd
    role: snmptrapd
  namespace: performance-idc   // namespace in which you want to deploy
the pod
spec:
  containers:
  - name: snmptrapd
    image: occne-repo-host:5000/snmptrapd:1.1.1  // you need to create you
own snmptrapd image using dockerfile
    volumeMounts:
      - name: config-volume
        mountPath: /MIB
```

```
    imagePullPolicy: IfNotPresent
    command: ["/bin/bash","-c","kill -9 $(lsof -t -i:162); cp /MIB/* /usr/
share/snmp/mibs && echo MIB files copied successfully ;snmptrapd -m ALL -f
-Of -Lo"]
    ports:
    - containerPort: 162
      protocol: UDP
    resources:
      limits:
        cpu: "1"
        memory: 1Gi
      requests:
        cpu: "1"
        memory: 1Gi
  volumes:
  - name: config-volume
    configMap:
      name: my-config
```

4. Run the following commands to deploy the service and pod in the SNMP Client:

   ```
   kubectl apply -f snmp-pod.yaml


   kubectl apply -f snmp-svc.yam
   ```

5. Run the following command to view the pod logs:

   ```
   $ kubectl logs pod/snmptrapd -n performance-idc
   ```

   Sample of the pod logs:

   ```
   kill: usage: kill [-s sigspec | -n signum | -sigspec] pid | jobspec ... or
   kill -l [sigspec]
   MIB files copied successfully
   NET-SNMP version 5.7.2
   ```

Integrate the Alert Manager with snmp-notifier Service

Update the SNMP client destination in *occne-snmp-notifier* service with the SNMP destination client IP:

```
$ kubectl edit deployment -n occne-infra occne-snmp-notifier
```

Update the field `--snmp.destination=<IP>:<port>` inside the args of container and add the *snmp-client* destination IP as follows:

```
- --snmp.destination=<fqdn of target receiver>:162
```

Verify the Traps

Run the following command to verify the traps:

```
$ kubectl logs pod/snmptrapd -n performance-idc -f
```

Sample output:

```
2024-03-11 11:31:10 10-233-87-165.occne-snmp-notifier.occne-infra.svc.blurr8
[UDP: [10.233.87.165]:46951->[10.233.116.34]:162]:
.iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.sysUpTimeInstance =
Timeticks: (147060000) 17 days,
0:30:00.00        .iso.org.dod.internet.snmpV2.snmpModules.snmpMIB.snmpMIBObje
cts.snmpTrap.snmpTrapOID.0 =
OID: .iso.org.dod.internet.private.enterprises.tekelecCorp.tekelecProductGroup
s.tekelecSwitchingGroup.oracleNWDAF.oracleNWDAFMIB.ocnwdafGeoredagent.ocnwdafg
eoredagentSvcDown     .iso.org.dod.internet.private.enterprises.tekelecCorp.te
kelecProductGroups.tekelecSwitchingGroup.oracleNWDAF.oracleNWDAFMIB.ocnwdafGeo
redagent.ocnwdafgeoredagentSvcDown.1 = STRING:
"1.3.6.1.4.1.323.5.3.45.1.33.2002[job=ocn-nwdaf-
georedagent]"        .iso.org.dod.internet.private.enterprises.tekelecCorp.tek
elecProductGroups.tekelecSwitchingGroup.oracleNWDAF.oracleNWDAFMIB.ocnwdafGeor
edagent.ocnwdafgeoredagentSvcDown.2 = STRING:
"critical"  .iso.org.dod.internet.private.enterprises.tekelecCorp.tekelecProdu
ctGroups.tekelecSwitchingGroup.oracleNWDAF.oracleNWDAFMIB.ocnwdafGeoredagent.o
cnwdafgeoredagentSvcDown.3 = STRING: "Status: critical
- Alert: OCN_NWDAF_GEOREDAGENT_NOT_RUNNING
  Summary: Service is down.
  Description: Service has been down for more than 2 minutes."
2024-03-11 11:35:38 10-233-87-165.occne-snmp-notifier.occne-infra.svc.blurr8
[UDP: [10.233.87.165]:56385->[10.233.116.34]:162]:
.iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.sysUpTimeInstance =
Timeticks: (147086800) 17 days,
0:34:28.00        .iso.org.dod.internet.snmpV2.snmpModules.snmpMIB.snmpMIBObje
cts.snmpTrap.snmpTrapOID.0 =
OID: .iso.org.dod.internet.private.enterprises.tekelecCorp.tekelecProductGroup
s.tekelecSwitchingGroup.oracleNWDAF.oracleNWDAFMIB.cap4cModelController.ocnwda
fcap4cModelControllerSvcDown  .iso.org.dod.internet.private.enterprises.tekele
cCorp.tekelecProductGroups.tekelecSwitchingGroup.oracleNWDAF.oracleNWDAFMIB.ca
p4cModelController.ocnwdafcap4cModelControllerSvcDown.1 = STRING:
"1.3.6.1.4.1.323.5.3.45.1.24.2002[job=cap4c-model-
controller]"    .iso.org.dod.internet.private.enterprises.tekelecCorp.tekelecP
roductGroups.tekelecSwitchingGroup.oracleNWDAF.oracleNWDAFMIB.cap4cModelContro
ller.ocnwdafcap4cModelControllerSvcDown.2 = STRING:
"critical"        .iso.org.dod.internet.private.enterprises.tekelecCorp.tekele
cProductGroups.tekelecSwitchingGroup.oracleNWDAF.oracleNWDAFMIB.cap4cModelCont
roller.ocnwdafcap4cModelControllerSvcDown.3 = STRING: "Status: critical
- Alert: CAP4C_MODEL_CONTROLLER_NOT_RUNNING
  Summary: Service is down.
  Description: Service has been down for more than 2 minutes."
```

Figure 10-2 Prometheus GUI

OCNWDAF MIB Files

Two OCNWDAF MIB files are used to generate the traps. The operator has to update the MIB files and the alert manager file to obtain the traps in their environment. The files are:

- *OCNWDAF-MIB-TC-24.2.0.mib*: This is a top level mib file, where the objects and their data types are defined.
- *OCNWDAF-MIB-24.2.0.mib*: This file fetches the objects from the top level mib file and based on the alert notification, the objects are selected for display.

OID Definition for OCNWDAF Services

OCNWDAF microservices and OID definitions are listed below:

OCNWDAF's OID: 1.3.6.1.4.1.323.5.3.45

Table 10-1 OID Definitions

Service Name	OID
cap4c-api-gateway	1.3.6.1.4.1.323.5.3.45.1.20
cap4c-capex-optimization-service	1.3.6.1.4.1.323.5.3.45.1.21
cap4c-configuration-manager-service	1.3.6.1.4.1.323.5.3.45.1.22
cap4c-kafka-ingestor	1.3.6.1.4.1.323.5.3.45.1.23
cap4c-model-controller	1.3.6.1.4.1.323.5.3.45.1.24
cap4c-stream-analytics	1.3.6.1.4.1.323.5.3.45.1.25
cap4c-stream-transformer	1.3.6.1.4.1.323.5.3.45.1.26
nwdaf-cap4c-reporting-service	1.3.6.1.4.1.323.5.3.45.1.27
nwdaf-cap4c-scheduler-service	1.3.6.1.4.1.323.5.3.45.1.28
nwdaf-cap4c-spring-cloud-config-server	1.3.6.1.4.1.323.5.3.45.1.29
ocn-nwdaf-analytics-info	1.3.6.1.4.1.323.5.3.45.1.30
ocn-nwdaf-data-collection-service	1.3.6.1.4.1.323.5.3.45.1.31
ocn-nwdaf-datacollection-controller	1.3.6.1.4.1.323.5.3.45.1.32
ocn-nwdaf-georedagent	1.3.6.1.4.1.323.5.3.45.1.33
ocn-nwdaf-mtlf-service	1.3.6.1.4.1.323.5.3.45.1.34
ocn-nwdaf-subscription-service	1.3.6.1.4.1.323.5.3.45.1.35

Alerts

OCNWDAF Subscription Alerts

This section lists the OCNWDAF subscription alerts:

Table 10-2 OCNWDAF_SUBSCRIPTION_CREATE

Field	Details
Severity	Info
OID to be appended	2000
Description	Indicates the subscription is successfully created.

Table 10-3 OCNWDAF_SUBSCRIPTION_CREATE_FAILURE

Field	Details
Severity	Warning
OID to be appended	2001
Description	Indicates an issue in creating the subscription.

Table 10-4 OCNWDAF_SUBSCRIPTION_DELETE

Field	Details
Severity	Info
OID to be appended	2002
Description	Indicates the subscription is successfully deleted.

Table 10-5 OCNWDAF_SUBSCRIPTION_UPDATE

Field	Details
Severity	Info
OID to be appended	2003
Description	Indicates the subscription is successfully updated.

Table 10-6 OCNWDAF_SUBSCRIPTION_DELETE_FAILURE

Field	Details
Severity	Warning
OID to be appended	2004
Description	Indicates an issue in deleting the subscription.

Table 10-7 OCNWDAF_SUBSCRIPTION_UPDATE_FAILURE

Field	Details
Severity	Warning
OID to be appended	2005
Description	Indicates an issue in updating the subscription.

Notification Alerts

This section lists the notification alerts:

Table 10-8 OCNWDAF_ABNORMAL_BEHAVIOR_STATISTICS_NOTIFICATION

Field	Details
Severity	Info
OID to be appended	3000
Description	Indicates abnormal behavior statistics notification is received.

Table 10-9 OCNWDAF_ABNORMAL_BEHAVIOR_THRESHOLD_NOTIFICATION

Field	Details
Severity	Info
OID to be appended	3001
Description	Indicates abnormal behavior threshold notification is received.

Table 10-10 OCNWDAF_ABNORMAL_BEHAVIOR_PREDICTION_NOTIFICATION

Field	Details
Severity	Info
OID to be appended	3002
Description	Indicates abnormal behavior prediction notification is received.

Table 10-11 OCNWDAF_NETWORK_PERFORMANCE_STATISTICS_NOTIFICATION

Field	Details
Severity	Info
OID to be appended	3003
Description	Indicates network performance statistics notification is received.

Table 10-12 OCNWDAF_NETWORK_PERFORMANCE_THRESHOLD_NOTIFICATION

Field	Details
Severity	Info
OID to be appended	3004
Description	Indicates network performance threshold notification is received.

Table 10-13 OCNWDAF_NETWORK_PERFORMANCE_PREDICTION_NOTIFICATION

Field	Details
Severity	Info
OID to be appended	3005
Description	Indicates network performance prediction notification is received.

Table 10-14 OCNWDAF_NF_LOAD_STATISTICS_NOTIFICATION

Field	Details
Severity	Info
OID to be appended	3006
Description	Indicates NF load statistics notification is received.

Table 10-15 OCNWDAF_NF_LOAD_THRESHOLD_NOTIFICATION

Field	Details
Severity	Info
OID to be appended	3007
Description	Indicates NF load threshold notification is received.

Table 10-16 OCNWDAF_NF_LOAD_PREDICTION_NOTIFICATION

Field	Details
Severity	Info
OID to be appended	3008
Description	Indicates NF load prediction notification is received.

Table 10-17 OCNWDAF_SLICE_LOAD_STATISTICS_NOTIFICATION

Field	Details
Severity	Info
OID to be appended	3009
Description	Indicates slice load statistics notification is received.

Table 10-18 OCNWDAF_SLICE_LOAD_THRESHOLD_NOTIFICATION

Field	Details
Severity	Info
OID to be appended	3010
Description	Indicates slice load threshold notification is received.

Table 10-19 OCNWDAF_SLICE_LOAD_PREDICTION_NOTIFICATION

Field	Details
Severity	Info
OID to be appended	3011
Description	Indicates slice load prediction notification is received.

ML Model Alerts

This section lists the ML model alerts:

Table 10-20 OCNWDAF_MODEL_CREATION_FAILURE

Field	Details
Severity	Critical
OID to be appended	4000
Description	Indicates an issue in ML model creation.

Table 10-21 OCNWDAF_MODEL_CREATION_SUCCESS

Field	Details
Severity	Info
OID to be appended	4001
Description	Indicates ML model is successfully created.

Data Collection Alerts

This section lists the data collection alerts:

Table 10-22 PRESENCE_IN_AOI_REPORT_RECEIVED

Field	Details
Severity	Info
OID to be appended	5000
Description	Indicates Presence in AOI report is successfully received.

Table 10-23 LOCATION_REPORT_RECEIVED

Field	Details
Severity	Info
OID to be appended	5001
Description	Indicates location report is successfully received.

Table 10-24 UES_IN_AREA_REPORT_RECEIVED

Field	Details
Severity	Info
OID to be appended	5002
Description	Indicates UEs in area report is successfully received.

Table 10-25 NF_LOAD_REPORT_RECEIVED

Field	Details
Severity	Info
OID to be appended	5003

Table 10-25 (Cont.) NF_LOAD_REPORT_RECEIVED

Field	Details
Description	Indicates NF load report is successfully received.

Table 10-26 SMF_SES_EST_REPORT_RECEIVED

Field	Details
Severity	Info
OID to be appended	5004
Description	Indicates a SMF session established report is successfully received.

Table 10-27 SMF_SES_REL_REPORT_RECEIVED

Field	Details
Severity	Info
OID to be appended	5005
Description	Indicates a SMF session released report is successfully received.

Table 10-28 KAFKA_SOURCED_REPORT_RECEIVED

Field	Details
Severity	Info
OID to be appended	5006
Description	Indicates Kafka sourced report is successfully received.

Operation Alerts

This section lists the operational alerts:

Table 10-29 OCN_NWDAF_SVC_HIGH_CPU_LOAD

Field	Details
Severity	Critical
OID to be appended	6000
Description	Verifies if the CPU usage of a particular service is exceeding 90%.

Table 10-30 OCN_NWDAF_SVC_HIGH_JVM_MEMORY_USAGE

Field	Details
Severity	Critical
OID to be appended	6001

Table 10-30 (Cont.) OCN_NWDAF_SVC_HIGH_JVM_MEMORY_USAGE

Field	Details
Description	Verifies if the percentage of heap memory used by a specific JVM instance/service is exceeding 90% over a one minute duration.

Table 10-31 OCN_NWDAF_SVC_NOT_RUNNING_ALERT

Field	Details
Severity	Critical
OID to be appended	6002
Description	Verifies if there are no instances of the specified service running in the specified Kubernetes namespace or if all instances of the service are not healthy.

10.2 System Level Alerts

This section lists the system level alerts.

OCN_NWDAF_ANALYTICS_HIGH_CPU_LOAD

Table 10-32 OCN_NWDAF_ANALYTICS_HIGH_CPU_LOAD

Field	Details
Description	CPU load is high at the pod where the microservice is running.
Affected Functions	All
Cause	CPU load is more than 80% of the allocated resources.

OCN_NWDAF_COMMUNICATION_HIGH_CPU_LOAD

Table 10-33 OCN_NWDAF_COMMUNICATION_HIGH_CPU_LOAD

Field	Details
Description	CPU load is high at the pod where the microservice is running.
Affected Functions	All
Cause	CPU load is more than 80% of the allocated resources.

OCN_NWDAF_CONFIGURATION_SERVICE_HIGH_CPU_LOAD

Table 10-34 OCN_NWDAF_CONFIGURATION_SERVICE_HIGH_CPU_LOAD

Field	Details
Description	CPU load is high at the pod where the microservice is running.
Affected Functions	All
Cause	CPU load is more than 80% of the allocated resources.

OCN_NWDAF_DATA_COLLECTION_HIGH_CPU_LOAD

Table 10-35 OCN_NWDAF_DATA_COLLECTION_HIGH_CPU_LOAD

Field	Details
Description	CPU load is high at the pod where the microservice is running.
Affected Functions	All
Cause	CPU load is more than 80% of the allocated resources.

OCN_NWDAF_GATEWAY_HIGH_CPU_LOAD

Table 10-36 OCN_NWDAF_GATEWAY_HIGH_CPU_LOAD

Field	Details
Description	CPU load is high at the pod where the microservice is running.
Affected Functions	All
Cause	CPU load is more than 80% of the allocated resources.

OCN_NWDAF_MTLF_HIGH_CPU_LOAD

Table 10-37 OCN_NWDAF_MTLF_HIGH_CPU_LOAD

Field	Details
Description	CPU load is high at the pod where the microservice is running.
Affected Functions	All
Cause	CPU load is more than 80% of the allocated resources.

OCN_NWDAF_SUBSCRIPTION_HIGH_CPU_LOAD

Table 10-38 OCN_NWDAF_SUBSCRIPTION_HIGH_CPU_LOAD

Field	Details
Description	CPU load is high at the pod where the microservice is running.
Affected Functions	All
Cause	CPU load is more than 80% of the allocated resources.

OCN_NWDAF_ANALYTICS_HIGH_JVM_HEAP_MEMORY_USAGE

Table 10-39 OCN_NWDAF_ANALYTICS_HIGH_JVM_HEAP_MEMORY_USAGE

Field	Details
Description	The average of the memory heap usage is high.
Affected Functions	All
Cause	The heap memory usage is more than 80%.

OCN_NWDAF_COMMUNICATION_HIGH_JVM_HEAP_MEMORY_USAGE

Table 10-40 OCN_NWDAF_COMMUNICATION_HIGH_JVM_HEAP_MEMORY_USAGE

Field	Details
Description	The average of the memory heap usage is high.
Affected Functions	All
Cause	The heap memory usage is more than 80%.

OCN_NWDAF_CONFIGURATION_SERVICE_HIGH_JVM_HEAP_MEMORY_USAGE

Table 10-41 OCN_NWDAF_CONFIGURATION_SERVICE_HIGH_JVM_HEAP_MEMORY_USAGE

Field	Details
Description	The average of the memory heap usage is high.
Affected Functions	All
Cause	The heap memory usage is more than 80%.

OCN_NWDAF_DATA_COLLECTION_HIGH_JVM_HEAP_MEMORY_USAGE

Table 10-42 OCN_NWDAF_DATA_COLLECTION_HIGH_JVM_HEAP_MEMORY_USAGE

Field	Details
Description	The average of the memory heap usage is high.
Affected Functions	All
Cause	The heap memory usage is more than 80%.

OCN_NWDAF_GATEWAY_HIGH_JVM_HEAP_MEMORY_USAGE

Table 10-43 OCN_NWDAF_GATEWAY_HIGH_JVM_HEAP_MEMORY_USAGE

Field	Details
Description	The average of the memory heap usage is high.
Affected Functions	All
Cause	The heap memory usage is more than 80%.

OCN_NWDAF_MTLF_HIGH_JVM_HEAP_MEMORY_USAGE

Table 10-44 OCN_NWDAF_MTLF_HIGH_JVM_HEAP_MEMORY_USAGE

Field	Details
Description	The average of the memory heap usage is high.
Affected Functions	All
Cause	The heap memory usage is more than 80%.

OCN_NWDAF_SUBSCRIPTION_HIGH_JVM_HEAP_MEMORY_USAGE

Table 10-45 OCN_NWDAF_SUBSCRIPTION_HIGH_JVM_HEAP_MEMORY_USAGE

Field	Details
Description	The average of the memory heap usage is high.
Affected Functions	All
Cause	The heap memory usage is more than 80%.

10.3 Application Level Alerts

This section lists the application level alerts.

OCN_NWDAF_ANALYTICS_NOT_RUNNING

Table 10-46 OCN_NWDAF_ANALYTICS_NOT_RUNNING

Field	Details
Description	The microservice is not available or not reachable.
Cause	Microservice ocn-nwdaf-analytics is down.

OCN_NWDAF_COMMUNICATION_NOT_RUNNING

Table 10-47 OCN_NWDAF_COMMUNICATION_NOT_RUNNING

Field	Details
Description	The microservice is not available or not reachable.
Cause	Microservice ocn-nwdaf-communication is down.

OCN_NWDAF_CONFIGURATION_SERVICE_NOT_RUNNING

Table 10-48 OCN_NWDAF_CONFIGURATION_SERVICE_NOT_RUNNING

Field	Details
Description	The microservice is not available or not reachable.
Cause	Microservice ocn-nwdaf-configuration-service is down.

OCN_NWDAF_DATA_COLLECTION_NOT_RUNNING

Table 10-49 OCN_NWDAF_DATA_COLLECTION_NOT_RUNNING

Field	Details
Description	The microservice is not available or not reachable.
Cause	Microservice ocn-nwdaf-data-collection is down.

OCN_NWDAF_GATEWAY_NOT_RUNNING

Table 10-50 OCN_NWDAF_GATEWAY_NOT_RUNNING

Field	Details
Description	The microservice is not available or not reachable.
Cause	Microservice ocn-nwdaf-gateway is down.

OCN_NWDAF_MTLF_NOT_RUNNING

Table 10-51 OCN_NWDAF_MTLF_NOT_RUNNING

Field	Details
Description	The microservice is not available or not reachable.
Cause	Microservice ocn-nwdaf-mtlf is down.

OCN_NWDAF_SUBSCRIPTION_NOT_RUNNING

Table 10-52 OCN_NWDAF_SUBSCRIPTION_NOT_RUNNING

Field	Details
Description	The microservice is not available or not reachable.
Cause	Microservice ocn-nwdaf-subscription is down.

HIGH_ABNORMAL_BEHAVIOUR_REQUEST_RATE

Table 10-53 HIGH_ABNORMAL_BEHAVIOUR_REQUEST_RATE

Field	Details
Description	The number of requests received per second is high.

Table 10-53 (Cont.) HIGH_ABNORMAL_BEHAVIOUR_REQUEST_RATE

Field	Details
Cause	Traffic is high, above 1000 requests per second.
URI Endpoint	`nnwdaf-analyticsinfo/v1/analytics?event-id=ABNORMAL_BEHAVIOUR`
Affected Functions	ABNORMAL_BEHAVIOUR

HIGH_UE_MOBILITY_REQUEST_RATE

Table 10-54 HIGH_UE_MOBILITY_REQUEST_RATE

Field	Details
Description	The number of requests received per second is high.
Cause	Traffic is high, above 1000 requests per second.
URI Endpoint	`nnwdaf-analyticsinfo/v1/analytics?event-id=UE_MOBILITY`
Affected Functions	UE_MOBILITY

HIGH_EVENT_SUBSCRIPTION_REQUEST_RATE

Table 10-55 HIGH_EVENT_SUBSCRIPTION_REQUEST_RATE

Field	Details
Description	The number of requests received per second is high.
Cause	Traffic is high, above 1000 requests per second.
URI Endpoint	`nnwdaf-eventssubscription/v1/subscriptions`
Affected Functions	UE_MOBILITY, SLICE_LOAD_LEVEL, ABNORMAL_BEHAVIOUR

HIGH_ABNORMAL_BEHAVIOUR_REQUEST_FAILURE_RATE

Table 10-56 HIGH_ABNORMAL_BEHAVIOUR_REQUEST_FAILURE_RATE

Field	Details
Description	The number of requests failing per second is high.
Cause	The request failing rate is more than the 70%.
URI Endpoint	`nnwdaf-analyticsinfo/v1/analytics?event-id=ABNORMAL_BEHAVIOUR`
Affected Functions	ABNORMAL_BEHAVIOUR

HIGH_UE_MOBILITY_REQUEST_FAILURE_RATE

Table 10-57 HIGH_ABNORMAL_BEHAVIOUR_REQUEST_FAILURE_RATE

Field	Details
Description	The number of requests failing per second is high.
Cause	The request failing rate is more than the 70%.
URI Endpoint	`nnwdaf-analyticsinfo/v1/analytics?event-id=UE_MOBILITY`
Affected Functions	UE_MOBILITY

HIGH_EVENT_SUBSCRIPTION_REQUEST_FAILURE_RATE

Table 10-58 HIGH_EVENT_SUBSCRIPTION_REQUEST_FAILURE_RATE

Field	Details
Description	The number of requests failing per second is high.
Cause	The request failing rate is more than the 70%.
URI Endpoint	`nnwdaf-eventssubscription/v1/subscriptions`
Affected Functions	UE_MOBILITY, SLICE_LOAD_LEVEL, ABNORMAL_BEHAVIOUR

10.4 OCNWDAF KPIs

This section provides information about Key Performance Indicators (KPIs) used for Oracle Communications Networks Data Analytics Function (OCNWDAF).

OCNWDAF KPIs are listed below:

Table 10-59 Frontend Reports Received Total

KPI Detail	Total number of reports received on Front End.
Metric Used for the KPI (CNE)	**PromQL:** total_fe_reports_recieved_total{namespace="$NAMESPACE"}
Metric Used for the KPI (OCI)	**MQL:**total_fe_reports_recieved_total[5m]{k8Namespace="$NAMESPACE"}.count()
Service Operation	NA
Response Code	NA
Tags and Values	Source NF: AMF,SMF,NRF,OAM

Table 10-60 Frontend Bytes Received Total

KPI Detail	Total number of bytes received on Front End.
Metric Used for the KPI (CNE)	**PromQL:** fe_bytes_recieved_total{namespace="$NAMESPACE"}

Table 10-60 (Cont.) Frontend Bytes Received Total

KPI Detail	Total number of bytes received on Front End.
Metric Used for the KPI (OCI)	**MQL:**fe_bytes_recieved_total[5m] {k8Namespace="$NAMESPACE"}.count()
Service Operation	NA
Response Code	NA
Tags and Values	Source NF: AMF,SMF,NRF,OAM

Table 10-61 Kafka Sourced Reports Received Total

KPI Detail	Total number of reports received by NWDAF Front End through Kafka.
Metric Used for the KPI (CNE)	**PromQL:** total_kafka_sourced_reports_recieved_total{namespace="$NAMESPACE"}
Metric Used for the KPI (OCI)	**MQL:**total_kafka_sourced_reports_recieved_total[5m]{k8Namespace="$NAMESPACE"}.count()
Service Operation	NA
Response Code	NA
Tags and Values	Source NF: OAM

Table 10-62 Total Kafka Bytes Received

KPI Detail	Total number of Kafka bytes received.
Metric Used for the KPI (CNE)	**PromQL:** total_kafka_bytes_recieved{namespace="$NAMESPACE"}
Metric Used for the KPI (OCI)	**MQL:**total_kafka_bytes_recieved[5m] {k8Namespace="$NAMESPACE"}.count()
Service Operation	NA
Response Code	NA
Tags and Values	Source NF: AMF,SMF,NRF,OAM Report Type: NW_PERF_OAM_REPORT, QOS_OAM_REPORT, UDC_OAM_REPORT

Table 10-63 Nwdaf Subscriptions Created Total

KPI Detail	Total number of subscriptions created.
Metric Used for the KPI (CNE)	**PromQL:** nwdaf_subscriptions_created_total{namespace="$NAMESPACE"}
Metric Used for the KPI (OCI)	**MQL:**nwdaf_subscriptions_created_total[5m] {k8Namespace="$NAMESPACE"}.count()
Service Operation	NA
Response Code	NA

Table 10-63 (Cont.) Nwdaf Subscriptions Created Total

KPI Detail	Total number of subscriptions created.
Tags and Values	Event Name: SLICE_LOAD_LEVEL, NETWORK_PERFORMANCE, NF_LOAD, ABNORMAL_BEHAVIOUR. Notification Method: DESCRIPTIVE, PREDICTIVE, THRSHOLDING.

Table 10-64 Nwdaf Subscriptions Accepted Total

KPI Detail	Total number of subscriptions accepted out of the subscriptions created.
Metric Used for the KPI (CNE)	**PromQL:** nwdaf_subscriptions_accepted_total{namespace="$NAMESPACE"}
Metric Used for the KPI (OCI)	**MQL:**nwdaf_subscriptions_accepted_total[5m]{k8Namespace="$NAMESPACE"}.count()
Service Operation	NA
Response Code	NA
Tags and Values	Event Name: SLICE_LOAD_LEVEL, NETWORK_PERFORMANCE, NF_LOAD, ABNORMAL_BEHAVIOUR. Notification Method: DESCRIPTIVE, PREDICTIVE, THRSHOLDING.

Table 10-65 Nwdaf Subscriptions Data Reports Sent

KPI Detail	Total number of reports or notifications sent.
Metric Used for the KPI (CNE)	**PromQL:** nwdaf_subscriptions_data_reports_sent_total{namespace="$NAMESPACE"}
Metric Used for the KPI (OCI)	**MQL:**nwdaf_subscriptions_data_reports_sent_total[5m]{k8Namespace="$NAMESPACE"}.count()
Service Operation	NA
Response Code	NA
Tags and Values	Event Name: SLICE_LOAD_LEVEL, NETWORK_PERFORMANCE, NF_LOAD, ABNORMAL_BEHAVIOUR. Notification Method: DESCRIPTIVE, PREDICTIVE, THRSHOLDING.

Table 10-66 Nwdaf Subscriptions Threshold Reports Sent

KPI Detail	Total number of threshold reports or notifications sent out of the total reports.
Metric Used for the KPI (CNE)	**PromQL:** nwdaf_subscriptions_threshold_reports_sent_total{namespace="$NAMESPACE"}

Table 10-66 (Cont.) Nwdaf Subscriptions Threshold Reports Sent

KPI Detail	Total number of threshold reports or notifications sent out of the total reports.
Metric Used for the KPI (OCI)	**MQL:**nwdaf_subscriptions_threshold_reports_sent_total[5m] {k8Namespace="$NAMESPACE"}.count()
Service Operation	NA
Response Code	NA
Tags and Values	Event Name: SLICE_LOAD_LEVEL, NETWORK_PERFORMANCE, NF_LOAD, ABNORMAL_BEHAVIOUR.

Table 10-67 Nwdaf Subscriptions Prediction Reports Sent

KPI Detail	Total number of predictive reports or notifications sent out of the total reports.
Metric Used for the KPI (CNE)	**PromQL:** nwdaf_subscriptions_prediction_reports_sent_total{namespace="$NAMESPACE"}
Metric Used for the KPI (OCI)	**MQL:**nwdaf_subscriptions_prediction_reports_sent_total[5m] {k8Namespace="$NAMESPACE"}.count()
Service Operation	NA
Response Code	NA
Tags and Values	Event Name: SLICE_LOAD_LEVEL, NETWORK_PERFORMANCE, NF_LOAD, ABNORMAL_BEHAVIOUR.

Table 10-68 Analyticsinfo Request Received Total

KPI Detail	Total number of analytics information requests received.
Metric Used for the KPI (CNE)	**PromQL:** analyticsinfo_request_received_total{namespace="$NAMESPACE"}
Metric Used for the KPI (OCI)	**MQL:**analyticsinfo_request_received_total[5m] {k8Namespace="$NAMESPACE"}.count()
Service Operation	NA
Response Code	NA
Tags and Values	Event Name: SLICE_LOAD_LEVEL, NETWORK_PERFORMANCE, NF_LOAD, ABNORMAL_BEHAVIOUR.