Oracle® Communications

Oracle Communications Networks Data Analytics Function User Guide

Release 22.1.0
F73272-01
December 2022

Oracle Communications Oracle Communications Networks Data Analytics Function User Guide, Release 22.1.0

F73272-01

Contents

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
CAP4C	Converged Analytics Platform for Communication
CNC	Cloud Native Core
CNE	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	Network Exposure Function
NF	Network Function
NRF	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	Network Slice Selection Function
OCNWDAF	Oracle Communications Networks Data Analytics Function
OAM	Operations, Administration, and Maintenance
PLMN	Public Land Mobile Network

Table (Cont.) Acronyms

Acronym	Description
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	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 22.1.0 in Oracle Communications Networks Data Analytics Function User Guide.

Release 22.1.0 - F73272-01, December 2022

- NF Load Analytics introduced
- Slice Load Level Analytics updated with new parameters

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 through an analytics function. The 5G technology requires prescriptive analytics to drive closed-loop automation and self-healing networks. In a 5G network, the consumers of data are 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. The data is collected directly from the NFs or through the Network Exposure Function (OCNEF).
- The OCNWDAF is designed to provide analytics information to consumer such as NFs, AFs and OAM.

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 data collected and analytics generated 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. This analytics information is used to balance the resources on the network. The OCNWDAF can predict the User Equipment (UE) location and also detect if the UE is in an abnormal location. Based on the collected 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 significantly fewer chances of network experiencing downtime.

An OCNWDAF consumer can avail analytics information for different analytic events. Alternatively, 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 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 types query the NRF and include the Analytics ID based on the required data.

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 Guide*
- *Oracle Communications Networks Data Analytics Function Troubleshooting Guide*
- *Oracle Communications Networks Data Analytics Function Disaster 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*

2
OCNWDAF Architecture

This chapter describes the OCNWDAF detailed design and architecture.

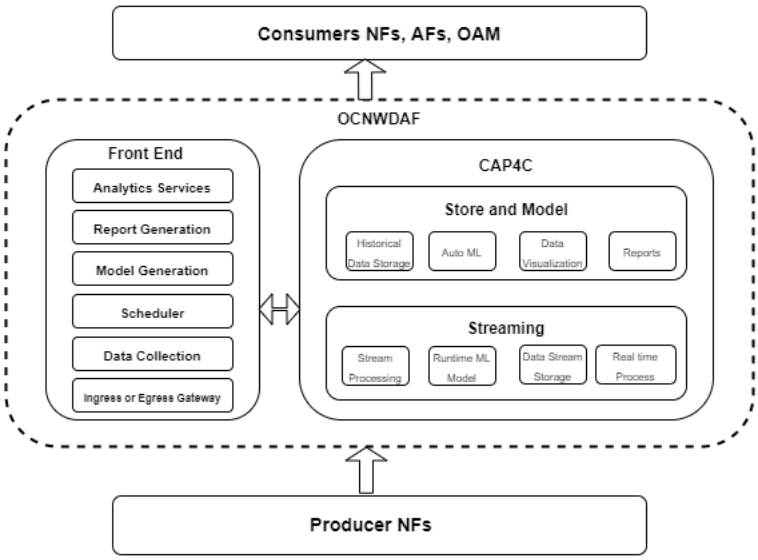
2.1 Oracle Communications Networks Data Analytics Function Architecture

OCNWDAF comprises of various microservices deployed in Kubernetes based Cloud Native Environment (CNE, example: OCCNE). The environment provides some common services such as logs or metrics data 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.

The microservices integrate with the environment and provide the necessary data.

The OCNWDAF architecture is depicted in the diagram below:

Figure 2-1 OCNWDAF Architecture



OCNWDAF Front End

- Collects data from 5G NFs
- Provides the data to backend CAP4C
- Collects the processed analytics information from CAP4C
- Provides the analytics information to the consumer NFs and AFs

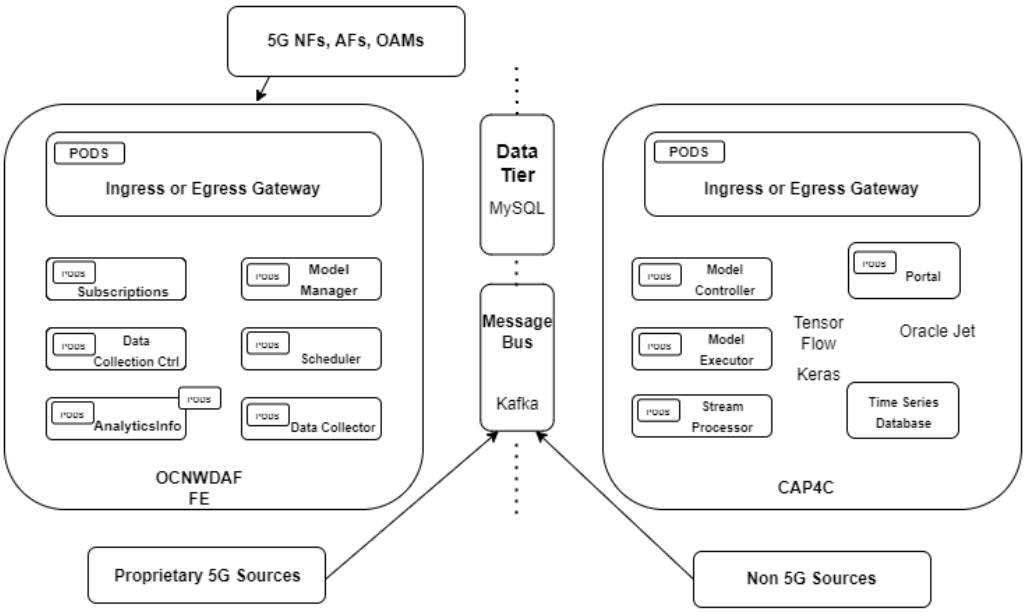
Converged Analytics Platform for Communication (CAP4C)

- Processes data from the Front End (FE)
- Examines streaming data in real time to enable thresholding and other uses
- Implements OCNWDAF analytics information (Statistical, Predictive, and Abnormal Behavior)
- Automates machine learning models
- Provides visualization and reports

2.2 Oracle Communications Networks Data Analytics Function Design

The OCNWDAF detailed design is depicted in the diagram below:

Figure 2-2 OCNWDAF Design



The OCNWDAF current architecture is aligned with 3GPP Release 16 but supports some common features in Release 17 such as Slice Load Level Analytics.

OCNWDAF Front End

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

Described below are the specialized OC-NWDAF microservices:

> **Note:**
>
> Some common services are also described below. The common services can be used by other 5G NFs along with OCNWDAF.

Ingress Gateway

The common Ingress gateway is refined to benefit from standard functionality such as ingress connection management, TLS1.2, and OAuth2.0

Egress Gateway

The common Egress gateway is refined to benefit from standard functionality such as egress connection management, including indirect communication, TLS1.2 and OAuth2.0, retry and reroute.

Scheduler

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

Model Manager

Tracks the consumer analytics requests, timeframe and data items required within the training data set to the respective ML models. Sends requests of models to be trained to the CAP4C and tracks the 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 network analytics subscription service sends analytics information 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. The network analytics information 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 are available.

Data Collection Service

For 3GPP 5G sources, the Data Collection service enables the OCNWDAF to retrieve data from various sources (for example, NFs such as AMF and SMF), this data is used for computation of network analytics. The Data Collection Service ensures the OCNWDAF efficiently obtains the appropriate data with the proper granularity.

The Data Collection Controller and Data Collector microservices together form the Data Collection Service of the OCNWDAF. Data is collected to generate predictive and descriptive analytics based on analyticsID. The OCNWDAF subscribes to (or cancels subscription) a Event ID (or set of Event IDs) by invoking the *Nnf_EventExposure_Subscribe* (or *Nnf_EventExposure_Unsubscribe*) service operation. If OCNWDAF subscribes to a Event ID (or set of EventIDs), the NFs notify the OCNWDAF by invoking *Nnf_EventExposure_Notify* service operation. For example, the NFs can notify the OCNWDAF with a event report.

- **Data Collection Control Service**: This service interacts with producer NFs to manage their subscriptions. This service also monitors and updates the consumers subscription information.
- **Data Collector Service**: This service receives data from the producer NFs and streams data to the CAP4C Analytics Engine.

Converged Analytics Platform for Communication (CAP4C)

The Analytics Engine (CAP4C) is the core of OCNWDAF, which supports data collection through the Front End (FE) module. The data collected is processed with the help of ML models. Predictive or descriptive data analysis is performed and data is transmitted through real-time stream processing.

Listed below are the OCNWDAF specific microservices (along with the common microservices):

- **Ingress and Egress Gateways**: In the OCNWDAF FE.
- **DBTier MySQL database**: Is used for general configuration, storage of microservice data (including dynamic state data) and ML models. Some specialized reports are also generated using the DBTier.
- **Time-Series database**: This database stores all the time-series data used for statistical reports and ML model datasets. Supports data roll-up (such as 1 up to 5 minute samples, 5 up to 15-minute samples, 15 minutes up to an hour sample and so on), allowing the storage of much older data in an efficient manner. Allows for fast and efficient data culling.
- **Kafka**: Is the internal messaging structure. 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 directs work to the Executor pool.
- **Model Executor**: Is a variable pool of resources that trains or executes models.
- **OCNWDAF Portal**: Performs the following functions:
  - Manages the OCNWDAF dashboards
  - Accepts operator input for configuration
  - Observes the time-series DB to change the display according to the change in the DB
  - Provides visualization of analytics information

3
OCNWDAF Features

This section explains the OCNWDAF features.

3.1 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 no intervention from the user.

For more information on installing and configuring ATS, see *Oracle Communications Cloud Native Core Automated Test Suite Guide*.

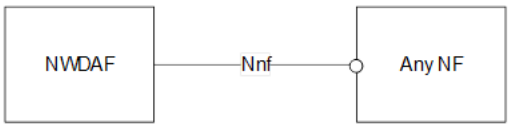
4
OCNWDAF Interfaces

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



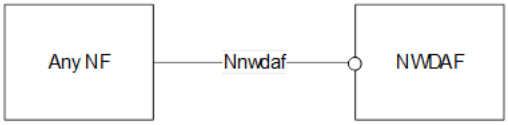
The OCNWDAF uses the *NnF* interface to:

- 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 Service

This service collects data from the sources listed below for different types of analytics:

- Global management data configured by the CSP.
- NFs data available in the 5G network.
- Data available in the individual NFs (for example, UE or UE group information).

The data collected is used as the basis for computing the analytics information. The data collection service handles the NF instance identification for the UEs and raises subscription requests to various NFs for NF data. It also receives notifications from the NFs for the subscribed events. This service enables the OCNWDAF to efficiently obtain appropriate data with the proper granularity. The operator can configure the OCNWDAF to collect analytics information from the NFs for future 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. The data collection service retrieves behavior data for individual UEs or groups of UEs and global UE information.

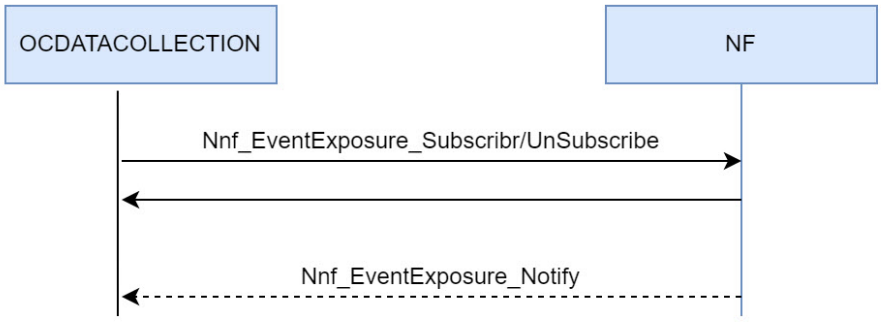
The collected data helps in computing predictive and descriptive analytics based on the AnalyticsID. Following AnalyticsIDs are supported:

- UE Mobility
- Slice Load Level
- Abnormal behavior (unexpected UE location)
- NF Load

Data Collection Procedure from NFs:

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

Figure 5-1 Data Collection from NFs



1. The Data Collection 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 of 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

Table 5-1 (Cont.) Exposure Services

Service producer	Service
UDM	Nudm_EventExposure
NEF	Nnef_EventExposure
NRF	Nnrf_NFDiscovery Nnrf_NFManagement

Data Collection by NRF

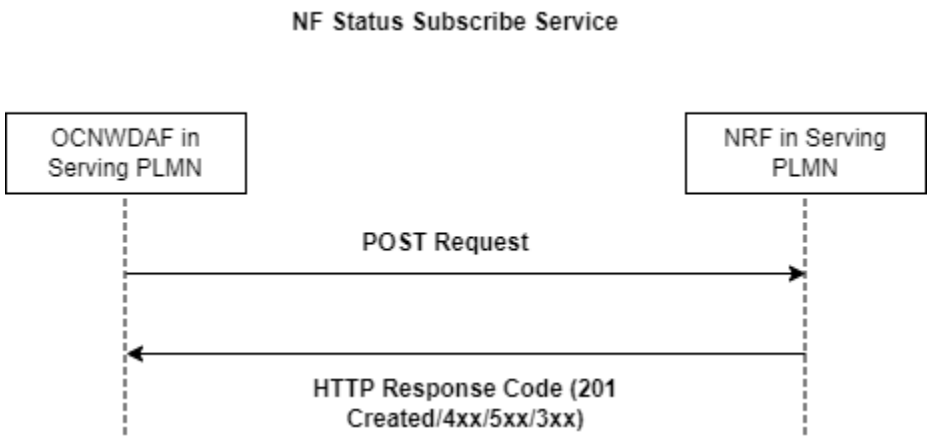
The OCNWDAF uses the NRF NF discovery service (*Nnrf_NFDiscovery*) to dynamically discover NF instances and their services in the 5G Core (5GC). This activity can be periodic or based on any specific event in the network. The OCNWDAF also utilizes the NRF MF Management Service (*Nnrf_NFManagement*), 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 5-2 NF Status Subscribe

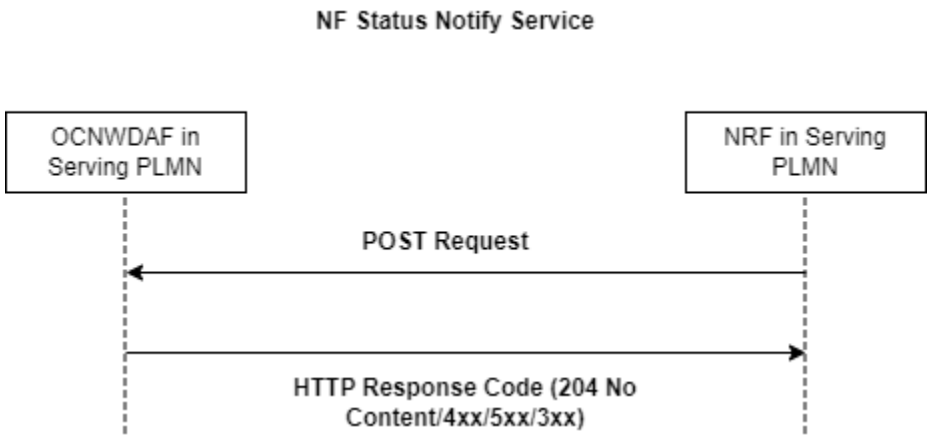


1. The OCNWDAF invokes the *NFStatusSubscribe* service to receive notifications about events (such as registration, deregistration, profile change) related to the Target NF located in the same PLMN by a POST request to the NRF.
2. The NRF authorizes or rejects the subscription request based on the validity 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 5-3 NF Status Notify

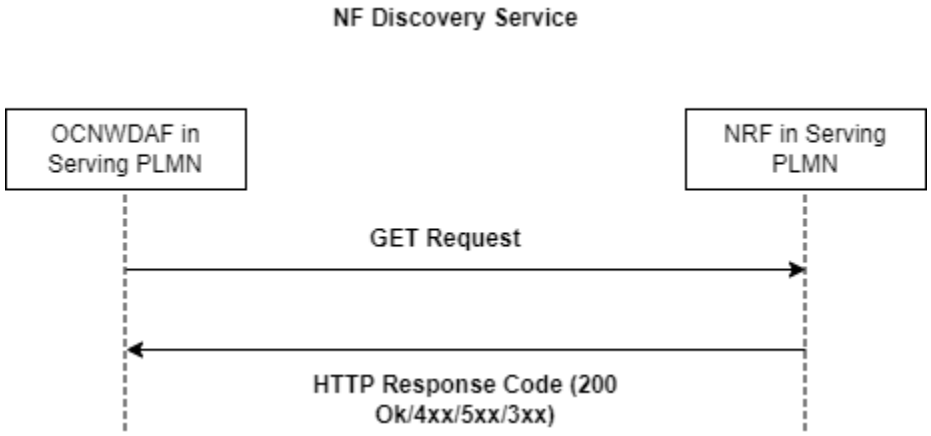


1. The NRF invokes the *NFStatusNotify* service POST request to the subscribed OCNWDAF to indicate any registration or profile changes in the target NF (or NF instances).
2. If the request is successful, the OCNWDAF responds with a "204 No content" HTTP response code.
3. If the request fails an appropriate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

5.4 Analytics Generation Service

The Analytics Generation service facilitates the generation of descriptive and predictive analytics provided by OCNWDAF. The service interfaces with the Data Collection service to obtain the raw data reports collected from different NFs and uses Analytics Engine (CAP4C) for the analytics processing.

In addition, the Analytics Generation service notifies the Analytics Subscription service about the generated analytics and obtains the generated analytics from either DBtier or Time Series Database. The service forms the core of OCNWDAF along with Data Collection and Analytics DB services. It is also responsible for interfacing with CAP4C to provision and fetch the trained ML models from the running Machine Learning Operations (MLOPs) service pipeline.

Also, the Analytics Generation service is responsible for performing features, such as managing subscription level aggregations, unrolling the raw data reports into a simple format, formatting the generated analytics into the OCNWDAF event notification format. In the case of complex descriptive analytics and predictions, the Analytics Generation service uses the backend Analytics Engine (CAP4C) data pipeline.

5.5 Analytics Database Service

The Analytics Database (DB) service communicates with the Analytics Information, Analytics Subscription, Data Collection, and Analytics Generation services for performing the following database operations:

- Storing or updating the analytics data into the analytics database

- Finding and deleting records from the analytics database

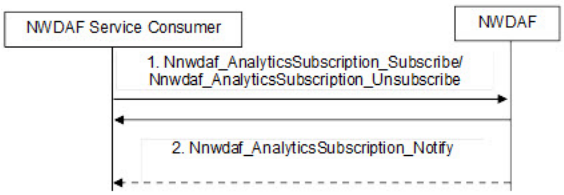
6
OCNWDAF Subscription and Analytics Requests

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

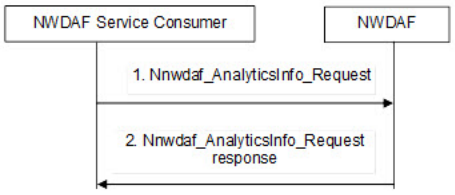


1. The OCNWDAF service consumer initiates or cancels a subscription to analytics information by invoking the *Nnwdaf_AnalyticsSubscription_Subscribe* or *Nnwdaf_AnalyticsSubscription_Unsubscribe* service operation. When a subscription to analytics information is received, the OCNWDAF determines whether 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

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

Correlation Information	Description
Timestamp, SUPI, DNN, S-NSSAI or UE IP address	To correlate data from SMF and PCF
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

An OCNWDAF consumer can avail analytics information or reports for various events in 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 assists in collecting and analysing data in a 5G 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. 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.

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

- Historical analytics
- Future analytics
- Reports when a thresholds are crossed
- Predictions on network behaviour and resource usage
- Prediction of abnormal events in the network

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 23.502 (version 3, table 4.15.1-1).
  - 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 "below", "above", 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.
  - An Analytics target period specified in past time is indicative of a analytics statistics request.
  - An Analytics target period specified in the future time is indicative of a 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 all the 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 information
- UE Abnormal Behaviour information
- NF Load Level analytics

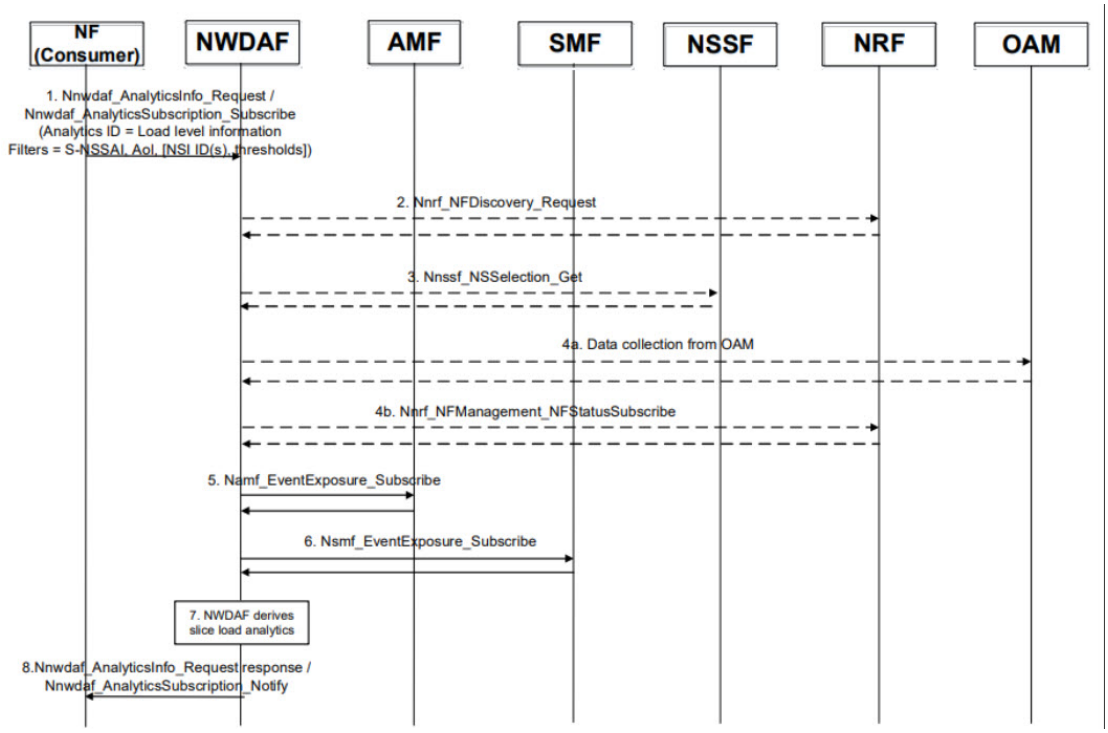
7.1 Slice Load Level Analytics

The OCNWDAF provides Slice Load Level analytics to the consumers at the Network Slice level, Network Slice instance level, or both. 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 7-1 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, NSI ID, Area of Interest and Load level threshold

value. The following steps are optional and applicable only if the nature of the requests matches the criterion listed below:

- The analytics request received by the OCNWDAF can be for historical or current data. If the OCNWDAF does not have the slice load information and the request is for historical data, it fetches the data from OAM. Suppose the request is for current data and OCNWDAF does not have the information, it performs an NRF discovery to discover AMF, SMF and NSSF instance(s) to fetch the relevant data based on the analytic filters provided in the analytics subscription service.
- If the consumer NF analytics subscription request does not contain the NSI ID(s), the OCNWDAF invokes *a Nnssf_NSSelection_Get* request to the NSSF to obtain the NSI ID(s) to the corresponding S-NSSAI in the subscription.
- The OCNWDAF can collect input data from the NRF to derive resource usage statistics and predictions for a Network Slice instance.

2. The OCNWDAF sends a *Namf_EventExposure_Subscribe* request to subscribe to the AMF's event exposure service. The OCNWDAF collects data on the number of UEs currently registered on the specific Network Slice (if the slice is available) and its constituent Network Slice instance(s). It also collects information on UEs access and mobility based on the event ID "UE moving in or out of Area of Interest". If the optional event Filters S-NSSAI, NSI ID(s) (if available), and Area of Interest are provided in the request, the OCNWDAF collects the corresponding UE IDs.
3. 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) and its constituent Network Slice instance(s). The PDU session establishment or release event information is collected.
4. The OCNWDAF derives the slice load analytics and delivers it to the consumers by invoking *OCNWDAF_AnalyticsSubscription_Notify* or *OCNWDAF_AnalyticsInfo_Request* response.

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 and NSI ID: The S-NSSAI is the network slice identifier. The use of NSI ID in the network is optional and depends on the deployment choices of the operator. If the NSI ID is specified, it is associated with S-NSSAI. The NSI ID is only applicable when the consumer is NSSF.
  - Area of Interest (AoI) (Optional)
  - Load level threshold value (Optional parameter, applicable only for Network Analytics Subscription Service)
  - List of NF types (Optional)
  - List of analytics subsets (Optional)
  - Maximum number of objects: When the Analytics Filter Information does not include the NSI ID, the "maximum number of objects" indicates the maximum

number of Network Slice instances expected in the output. It is an optional parameter.

The OCNWDAF reports when the load level of the network slice instance 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 7-1 Network Slice 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.

Table 7-1 (Cont.) Network Slice Load statistics

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 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.
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 7-2 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 7-3 Network Slice 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.
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.

Table 7-3 (Cont.) Network Slice Load Predictions

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.
Confidence	Uinteger	C	0 to 1	Indicates the confidence of this prediction. It has a value range from Minimum "0" up to Maximum "100".

7.2 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). For more information, see UE Abnormal Behavior Analytics.

The OCNWDAF service consumer may request for these analytics separately, or in a combined manner.

7.2.1 UE Mobility Analytics

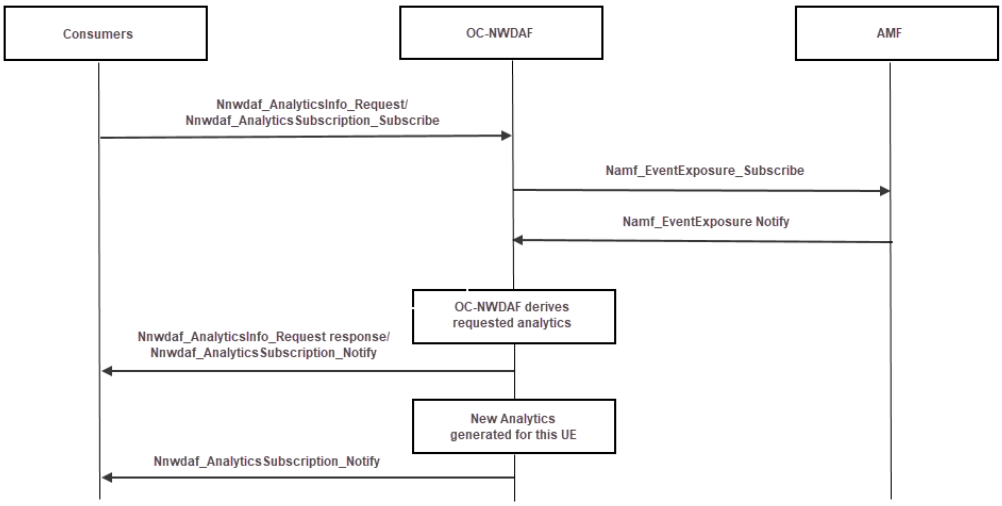
OCNWDAF provides UE mobility statistical or predictive analytics to allow consumers to do the following:

- 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 7-2 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.
4. OCNWDAF provides the requested UE mobility analytics to the consumer, using either *Nnwdaf_AnalyticsInfo_Request* response or *Nnwdaf_AnalyticsSubscription_Notify*, depending on the service used in step 1.

5. If at step 1, the consumer has subscribed to receive notifications for UE mobility analytics, after receiving event notification from the AMFs subscribed by OCNWDAF in step 2, OCNWDAF may generate new analytics and provide them to the NF.

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 7-4 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.
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.

Table 7-4 (Cont.) UE mobility descriptive analytics

Parameter	Data type	P	Cardinality	Description
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 7-5 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.
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.

Table 7-5 (Cont.) UE mobility predictive analytics

Parameter	Data type	P	Cardinality	Description
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.

7.2.2 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 behaviour, for example, misused or hijacked UEs.

Note:

The misused or hijacked UEs include the UEs in which there are malicious applications running or the UEs that are stolen.

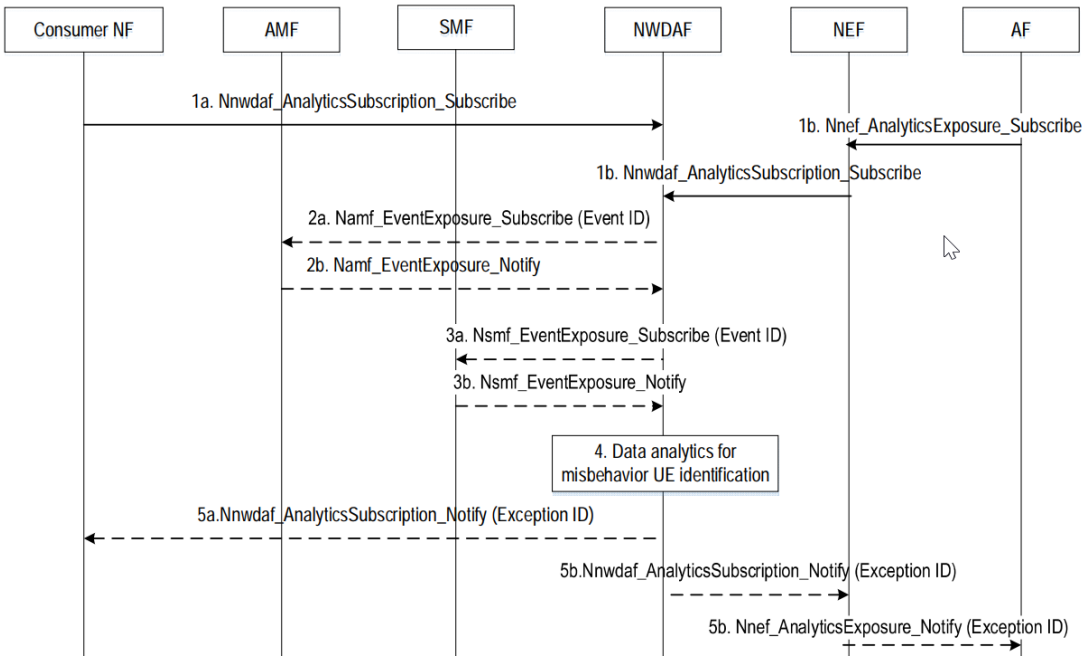
The UE abnormal behavior analytics consumer subscribes analytics about abnormal behaviour from OCNWDAF based on the UE subscription, network configuration, or application layer request.

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

> **Note:**
>
> In the current release only unexpected UE location is monitored, more aspects of UE abnormal behaviour and respective analytics are planned for future releases. (Such as Exception reports that result from the analysis of the correlations between behavioural variables. The exception reports contain an Exception Level expressed in the form of a scalar value, which is possibly supplemented by additional measurements.)

UE Abnormal Behavior Workflow

Figure 7-3 UE Abnormal Behavior Workflow



1. a. A consumer subscribes to or requests OCNWDAF using *Nnwdaf_AnalyticsSubscription_Subscribe* or *Nnwdaf_AnalyticsInfo_Request* (Analytics ID set to "Abnormal behaviour", Target of Analytics Reporting set to Internal-Group-Identifier, any UE or SUPI, Analytics Filter Information).
   A consumer NF may subscribe to or request abnormal behaviour notification or response from 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 behaviour analytics.

   b. AF to OCNWDAF: *Nnwdaf_AnalyticsSubscription_Subscribe* or *Nnwdaf_AnalyticsInfo_Request* (Analytics ID, Target of Analytics Reporting set to External-group identifier, any UE or External UE ID, Analytics Filter Information)
   For untrusted AFs, the AF sends the subscription through a NEF, where the AF invokes NEF service *Nnef_AnalyticsExposure_Subscribe* or *Nnef_AnalyticsExposure_Fetch* (Analytics ID, Target of Analytics Reporting set to External-group-identifier, any UE or External UE ID, Analytics Filter Information).

An AF may also subscribe to or request abnormal behaviour notification or response from OCNWDAF for a group of UEs, a specific UE or any UE, where the subscription or request message may contain expected UE behaviour parameters identified on the application layer. If an External-Group-Identifier is provided by the AF, the NEF interrogates UDM to map the External-Group-Identifier to the Internal-Group-Identifier and obtain SUPI list corresponding to the Internal-Group-Identifier.

2. OCNWDAF to AMF: *Namf_EventExposure_Subscribe* (Event ID(s), Event Filter(s), Internal-GroupIdentifier, any UE or SUPI).
OCNWDAF sends subscription requests to the related AMF to collect UE behavioural 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 behaviour matches its expected UE behavioural information. In this case, the AMF sends event reports to OCNWDAF only when it detects that the UE's behaviour deviated from its expected UE behaviour.

3. OCNWDAF performs data analytics for misused or hijacked UEs identification. Based on the analytics and operator's policies, OCNWDAF determines whether to send a notification to the consumer NF or AF.

4. a. OCNWDAF to consumers (AMF or PCF or SMF depending on the subscription): *Nnwdaf_AnalyticsSubscription_Notify* or *Nnwdaf_AnalyticsInfo_Response* (Analytics ID, Exception ID, Internal-Group-Identifier or SUPI, Exception level) (which is used depending on the service used in step 1a).
If OCNWDAF determines to send a notification or response to the consumer 5G NFs, OCNWDAF invokes *Nnwdaf_EventSubscription_Notify* or *Nnwdaf_AnalyticsInfo_Response* services. Based on the notification or response, the 5G NFs adopt configured actions to resolve/mitigate/avoid the risks.

> **Note:**
>
> - Based on the notification, the AF can adopt corresponding actions, for example, adjusting recommended TCP Window Size, adjusting recommended Service Start and End.

Consumer request to OCNWDAF

A consumer request for this analytics information contains:

- Analytics ID: “Abnormal Behavior”
- The following filters can be specified in the network analytics subscription service and network analytics information service:

- Single UE, a group of UEs (internal Group ID), or any UE
- Target time period of the request
- S-NSSAI (Optional)
- A Notification Correlation ID and Target Address in a subscription

Note:

- For UE mobility related abnormal behaviour analytics:
  - Either of the following parameters are set to indicate that the mobility related abnormal behaviour analytics are expected:
    - Expected analytics type
    - List of exception IDs
  - The analytics filter should at least include S-NSSAI (if the Target of Analytics Reporting is any UE)
- When OCNWDAF detects those UEs that deviate from the expected UE behaviour, for example, unexpected UE location, abnormal traffic pattern, or wrong destination address, OCNWDAF notifies the result of the analytics as specified in Output UE Abnormal Behavior Analytics.

Output UE Abnormal Behavior Analytics

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

Table 7-6 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.
Exception Level	Integer	O	0 to 1	Measured level, compared to the threshold
Exception trend	ExceptionTrend	O	0 to 1	Measured trend.
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

Table 7-6 (Cont.) UE abnormal behavior analytics

Parameter	Data type	Mandatory or Optional	Cardinality	Description
Ratio	SamplingRatio	C	0 to 1	Indicates the estimated percentage of the UEs affected by Exception within the target of analytics reporting
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.

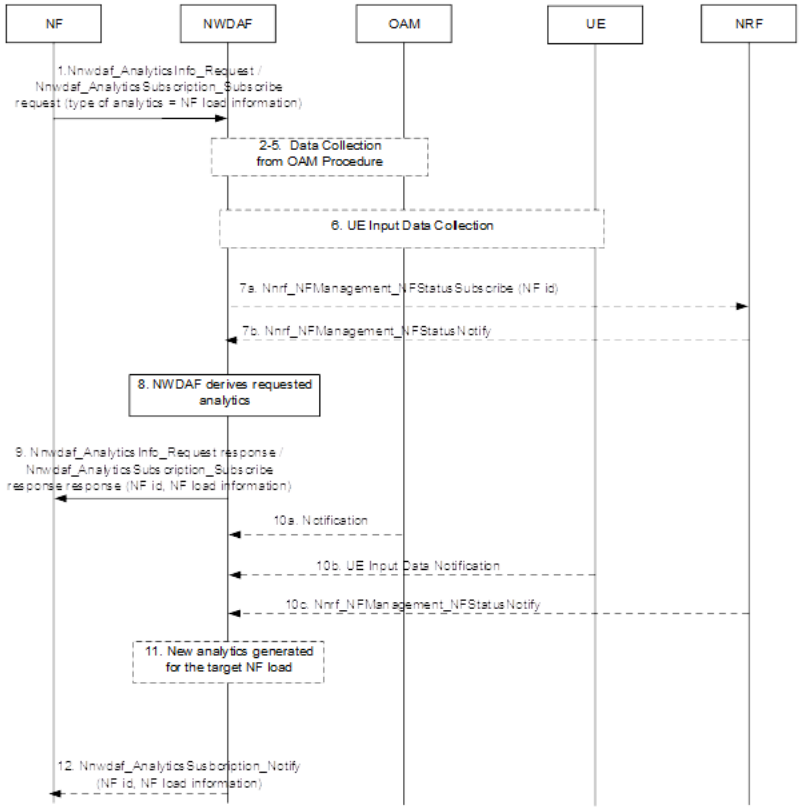
7.3 Network Function (NF) Load Analytics

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



> **Note:**
>
> Data collection from OAM is not supported in the current release.

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* or a *Nnwdaf_AnalyticsSubscription* 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.
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_Request* response or *Nnwdaf_AnalyticsSubscription_Subscribe* 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.

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 (an optional SUPI or "any UE"): Only AMF and SMF can be determined from the SUPI.
- Analytics filter information, consisting of the following:
  - S-NSSAI (optional)
  - Optional list of NF Instance IDs, NF Set IDs, or NF types
  - Area of Interest (AoI) (optional)
  - 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.

> **Note:**
>
> If a SUPI is provided as the target of analytics reporting, the OCNWDAF uses the SUPI to determine which NF instances (AMF and SMF) that are serving this specific UE and then filters them based on S-NSSAI and NF types using the data collected from NRF. NF load analytics are then provided based on these NF instances.

> **Note:**
>
> If a list of the NF Instance IDs (or respectively of NF Set IDs) is provided, the OCNWDAF provides the analytics for each designated NF instance (or respectively for each NF instance belonging to each designated NF Set). In this case, the SUPI (Target of Analytics Reporting) in the consumer request is ignored.

NF Load Data Collection

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

Table 7-7 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 7-8 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).

Table 7-8 (Cont.) NF Load Statistics

Parameter	Data Type	P	Cardinality	Description
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 7-9 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 7-10 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

Table 7-10 (Cont.) NFType

Enumeration Value	Description
"MB_SMF"	Network Function: MB-SMF
"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 7-11 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 7-12 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 7-13 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 7-14 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.

8
OCNWDAF Graphical User Interface (GUI)

This chapter describes the OCNWDAF Graphical User Interface (GUI).

8.1 OCNWDAF Login

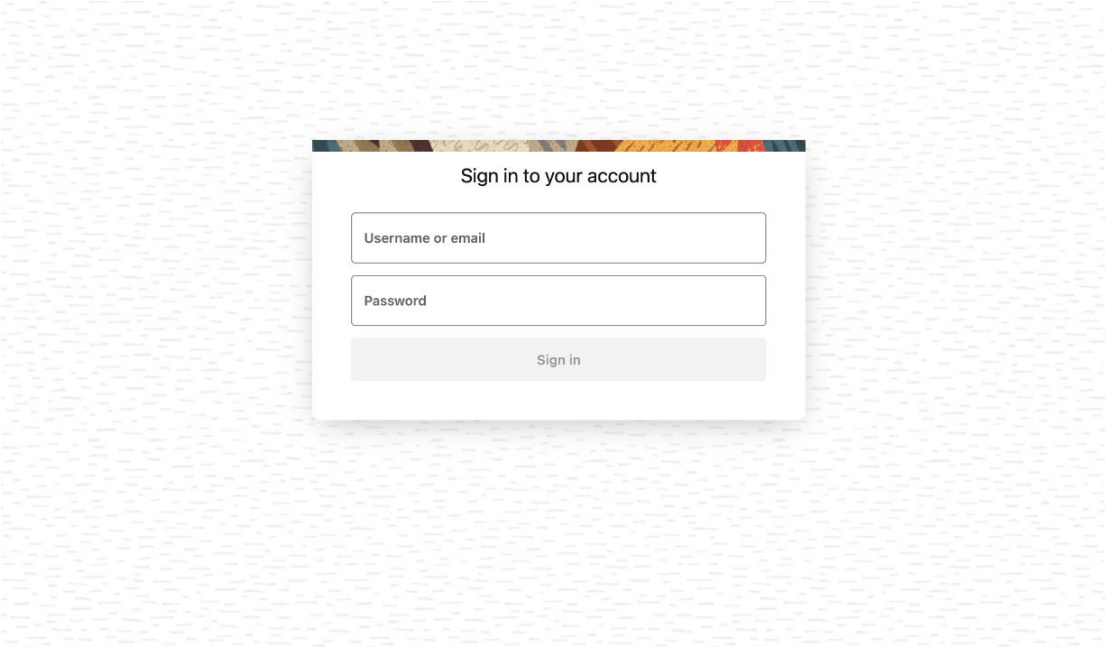
Log in to the OCNWDAF Graphical User Interface (GUI) using valid credentials. The OCNWDAF supports three kinds of users listed below:

- Network Operator
- Network Architect
- Network Capacity Planner

The Network Architect and Network Capacity Planner have access to the **Configuration** screen to add new slices, manage existing slices, modify slice settings and access geographical settings to create new regions.

Enter the Username and Password, and click **Sign in** to log in to the OCNWDAF application.

Figure 8-1 Login



After a successful login, the following **Network Overview** page appears on the screen.

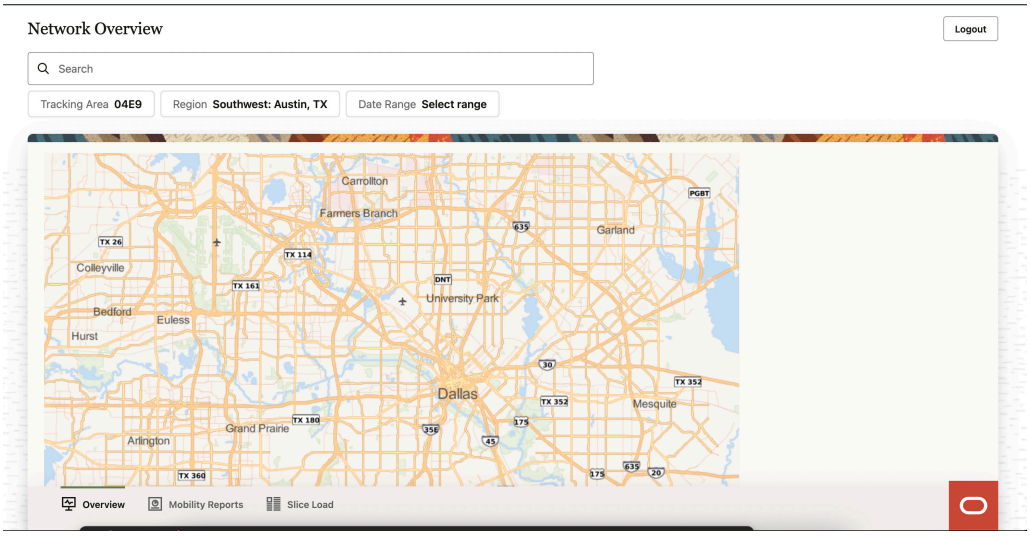
8.2 Network Overview Screen

The **Network Overview** displays the overview of the network and allows the user to perform the following actions:

- **Search**: A search bar is available with option to select the following filters:
  - **Tracking Area**
  - **Region**
  - **Date Range**
- **Logout**
- Generate **Mobility Reports**
- Obtain **Slice Load** analytics
- Access to the **Configuration** screen (only if the user is a Network Planner or Network Architect).

The following **Network Overview** screen is visible to the Network Operator:

Figure 8-2 Network Overview Screen



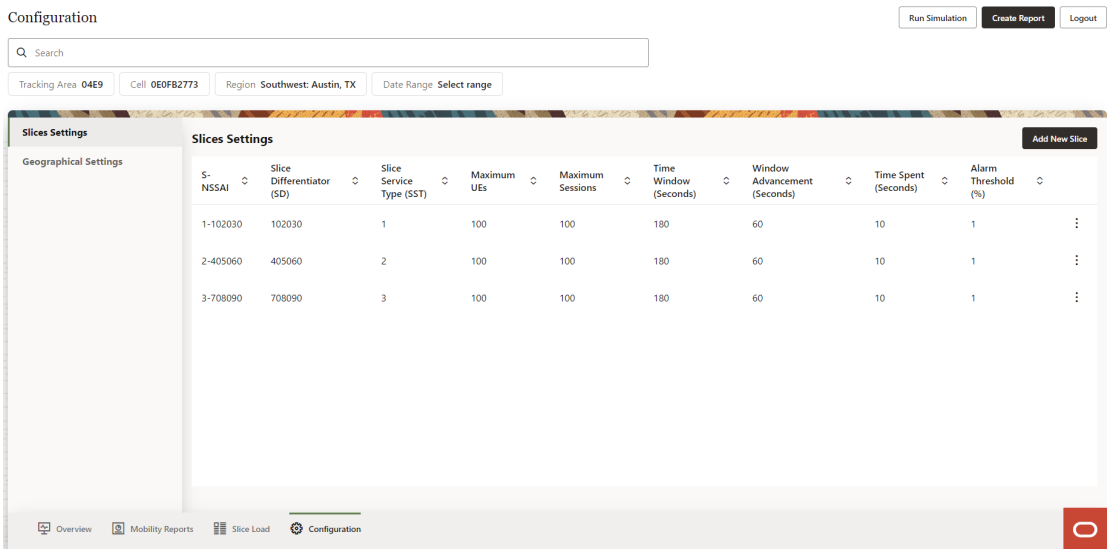
> **Note:**
>
> The Network Planner and Network Architect have access to the **Configuration** button on the screen.

8.3 OCNWDAF Configuration Page

To open the **Configuration** page, log in to the portal, the **Network Overview** screen appears. Click **Configuration** button at the bottom of the screen to open the **Configuration** page.

> **Note:**
>
> Access to the **Configuration** button in the **Network Overview** page is available only when the user logged in is a Network Planner or Network Architect. A Network Operator does not have access to the **Configuration** page.

Figure 8-3 Configuration Page



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

- Access the **Slice Settings**
- Access the **Geographical Settings**
- **Run Simulation**
- **Create Report**
- **Logout**
- Perform a search using the **Search** bar, by applying the following filters:
  - **Tracking Area**
  - **Cell**
  - **Region**
  - **Date Range**

8.3.1 Slice Setting Screen

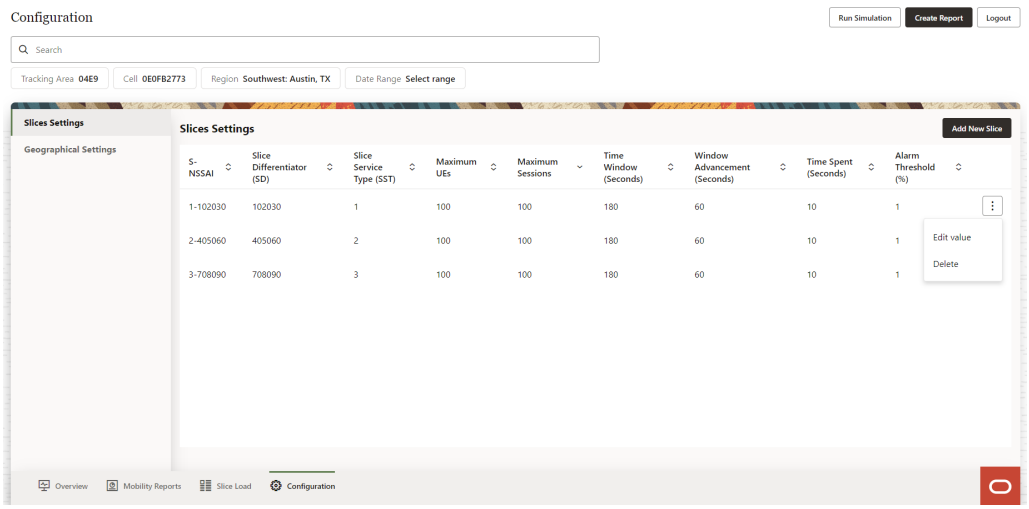
The **Configuration** screen displays the **Slice Settings** option. The user can perform the following actions on the **Slice Settings** screen:

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

  - **S-NSSAI**
  - **Slice Differentiator (SD)**
  - **Slice Service Type (SST)**
  - **Maximum UEs**
  - **Maximum Sessions**
  - **Time Window (Seconds)**
  - **Window Advancement (Seconds)**
  - **Time Spent (Seconds)**
  - **Alarm Threshold (%)**
- Modify existing slice information using the **Edit Value** button. This button appears as a pop up on clicking the three dot menu option on the right side of each configured slice listed on the screen.
- Delete an existing slice, using the **Delete** button. This button appears as a pop up on clicking the three dot menu option on the right side of each configured slice listed on the screen.

The **Slice Settings** screen is displayed below:

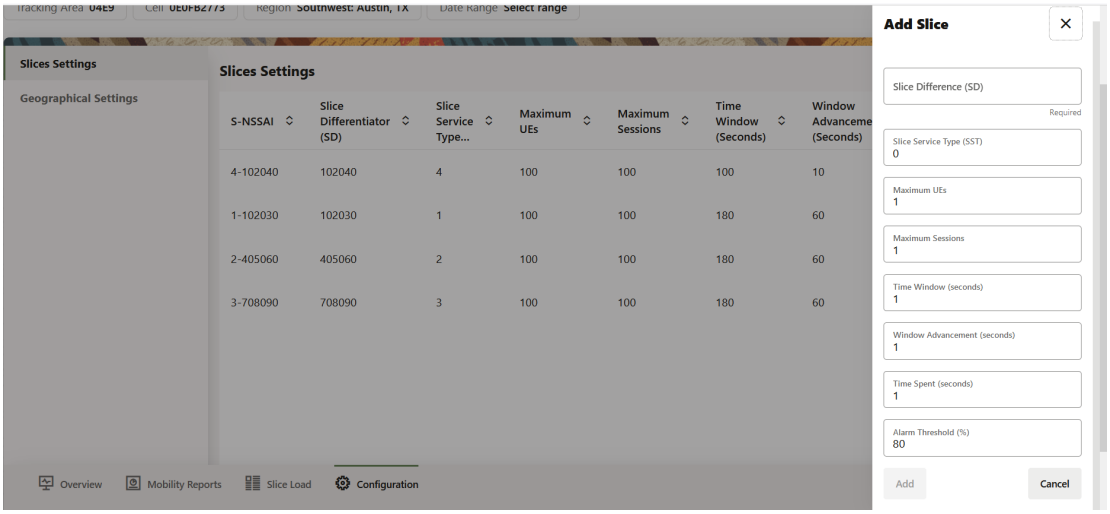
Figure 8-4 Slice Settings



8.3.1.1 Add a New Slice

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

Figure 8-5 Add Slice



Provide the following information to create a new slice:

Table 8-1 New Slice

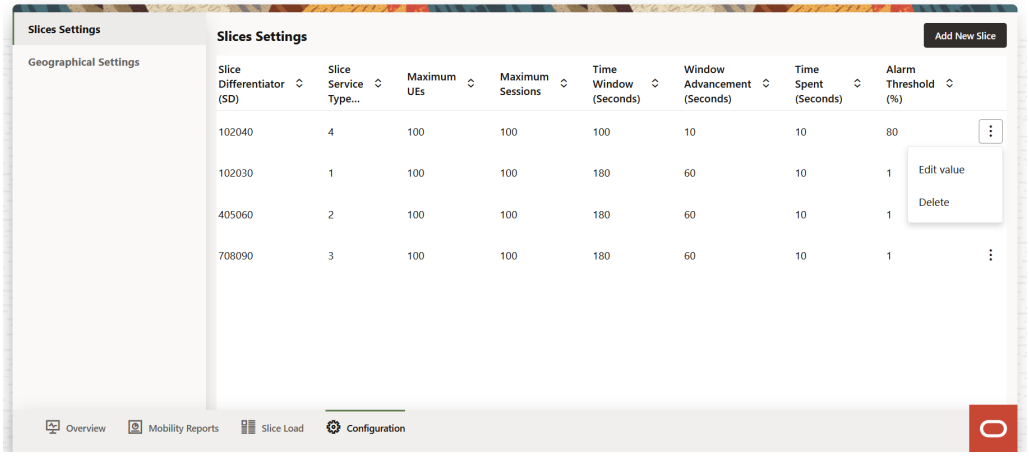
Parameter	Type	Description
Slice Difference (SD)	String	Is a 3-octet hexadecimal number to identify different slices of the same type.
Slice Service Type (SST)	Unsigned integer	Value: 0 up to 127 is standardized, and 128 up to 255 is operator specific.
Maximum UEs	Integer	The maximum number of user equipments allowed in the slice.
Maximum Sessions	Integer	The maximum number of sessions allowed in the slice.
Time Window	Seconds	Threshold detection window time. Default: 5 minutes.
Window Advancement	Seconds	Threshold detection window advancement. Default: 15 seconds.
Time Spent	Seconds	Time spent in window opposite accepted state. Default: 80% .
Alarm Threshold	Percentage	Indicates the value of the Alarm Threshold.

Click the **Add** button after entering all the fields to create a new slice. The new slice will be listed in the **Slice Settings** screen.

8.3.1.2 Delete a Slice

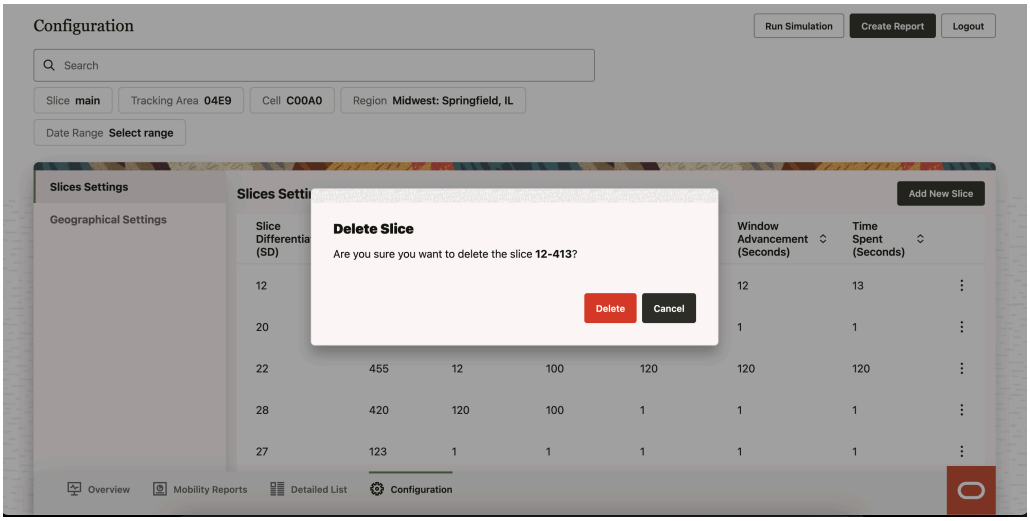
To delete a slice, click the three dot menu button on the right side of the slice to be deleted. A pop up appears which has an option to **Delete** slice.

Figure 8-6 Delete



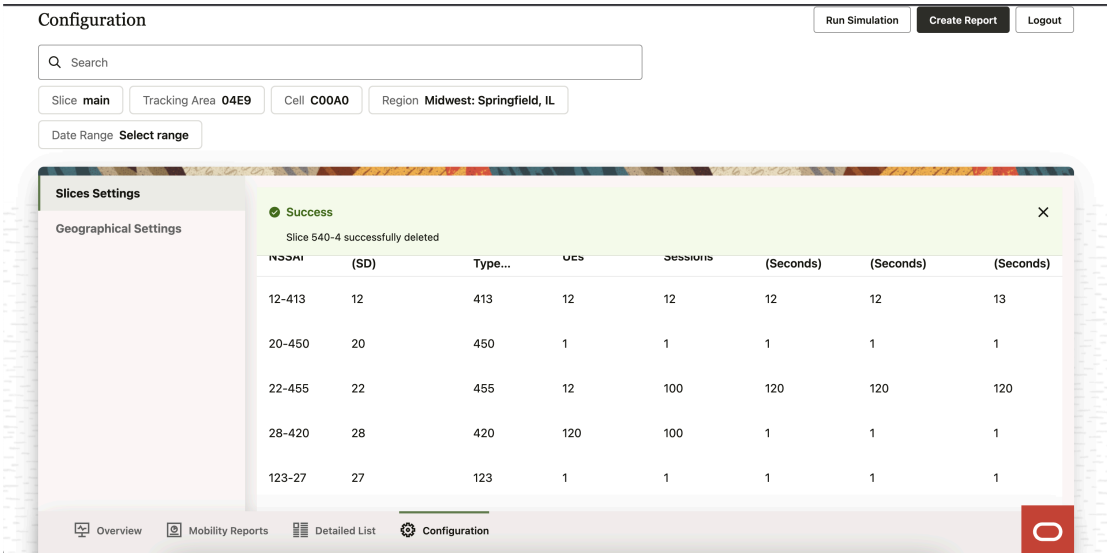
Click **Delete**, a Delete Slice confirmation dialog box appears on the screen. Click **Delete** to confirm deletion or **Cancel** to cancel slice deletion.

Figure 8-7 Confirm Delete



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

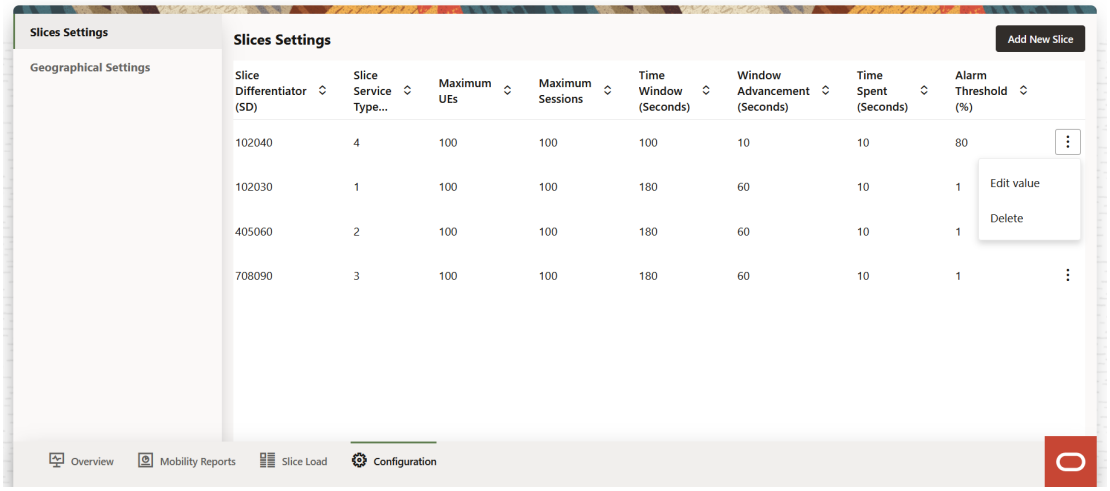
Figure 8-8 Successful Deletion



8.3.1.3 Edit an Existing Slice

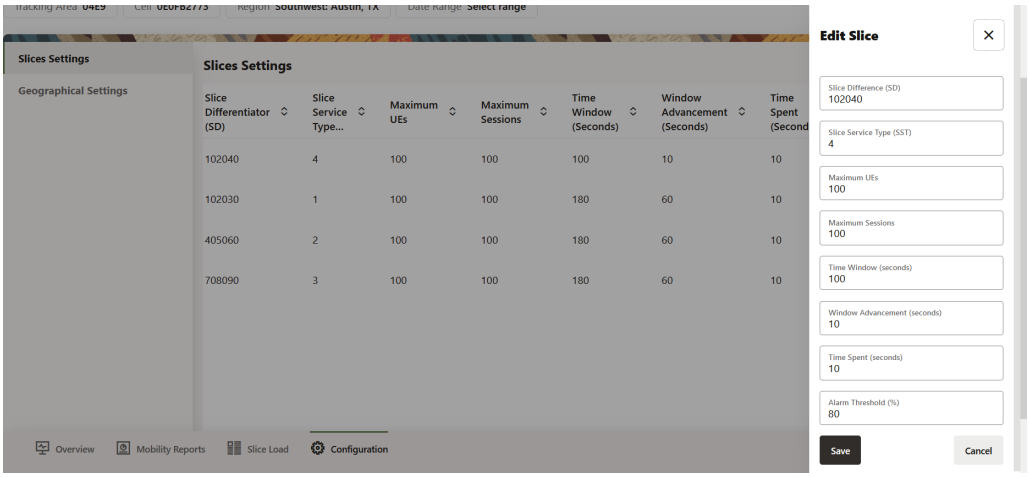
To edit a slice, click dotted menu button on the right side of the slice to be edited. Click the **Edit value** option that appears as a pop up on the screen.

Figure 8-9 Edit value



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

Figure 8-10 Edit Slice

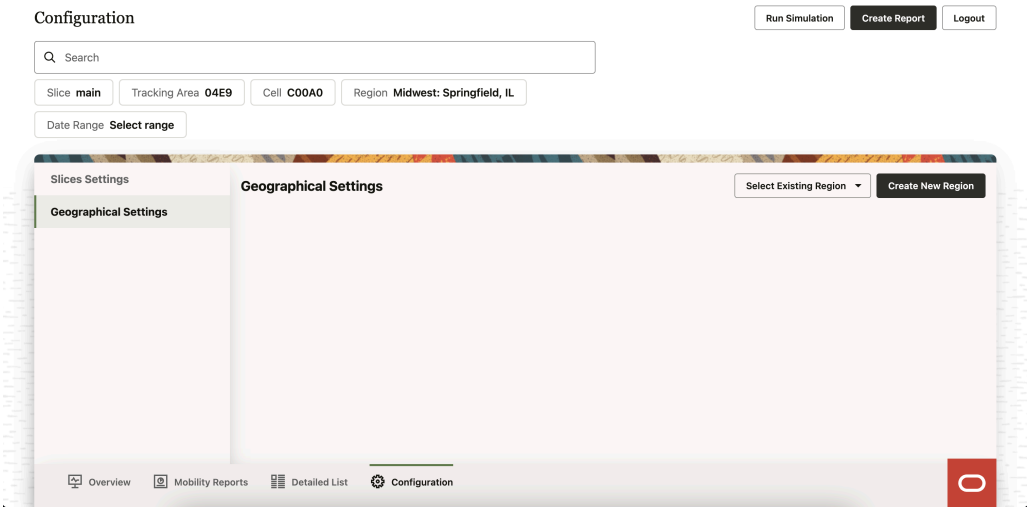


Modify the required fields to edit the slice. Click **Save** to apply the changes to the slice.

8.3.2 Geographical Settings

The **Configuration** screen displays the **Geographical Settings** option. Click on the **Geographical Settings** option on the left side of the screen. The **Geographical Settings** screen appears.

Figure 8-11 Geographical Settings

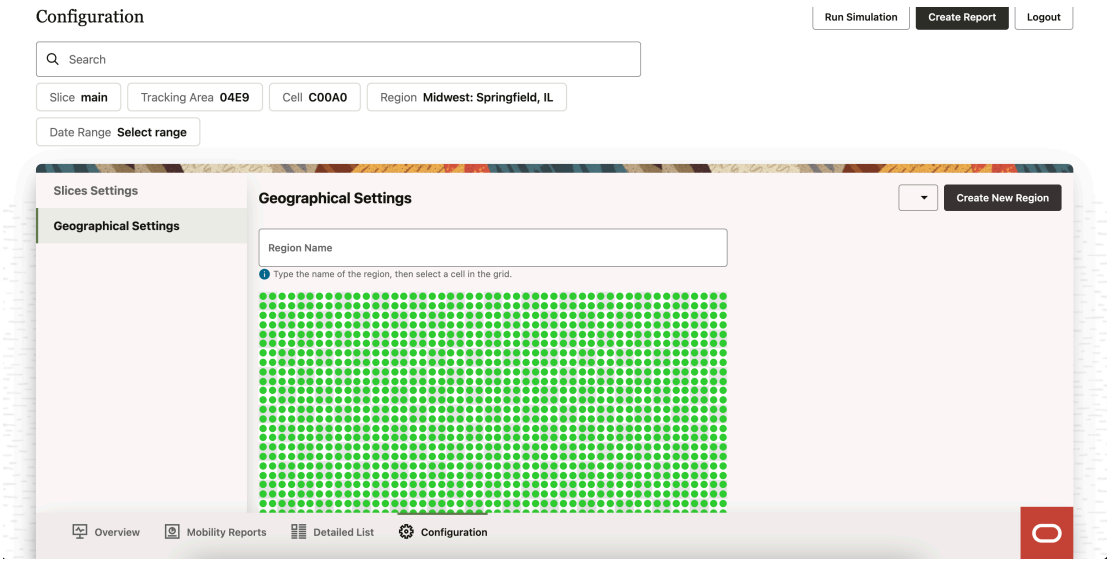


Use this screen to **Select Existing Region** or **Create New Region**.

8.3.2.1 Create New Region

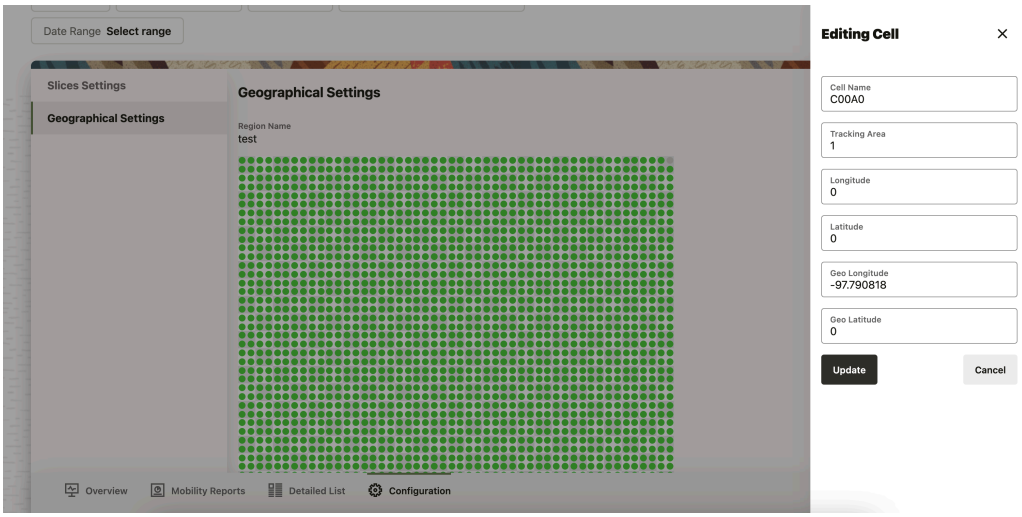
Click **Create New Region** to create a new region.

Figure 8-12 Create New Region



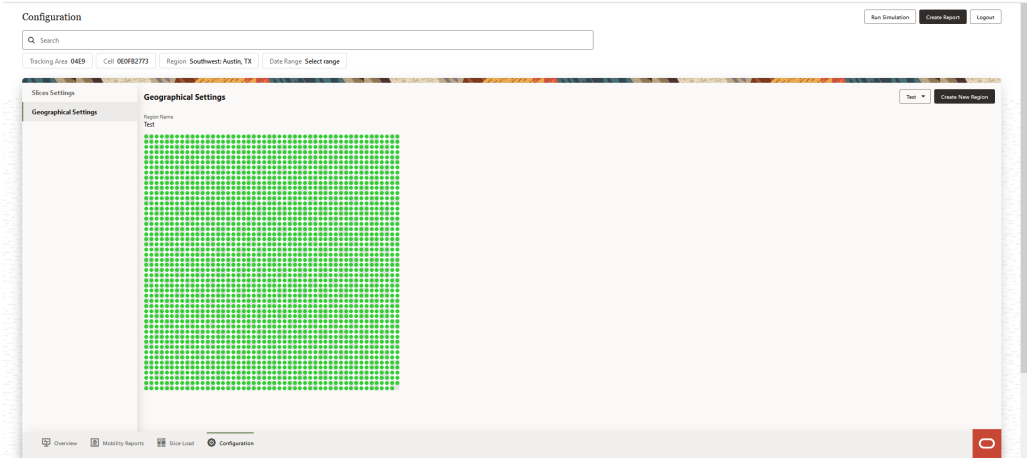
- Provide a **Region Name**, and then select the cell in the grid.
- The **Editing Cell** screen displays on the right side of the screen to update the region information. Provide the following details:
  - Cell Name
  - Tracking Area
  - Longitude
  - Latitude
  - Geo Longitude
  - Geo Latitude
- Click **Update** to save the changes.
- Click **Cancel** to discard the changes.

Figure 8-13 New Region Parameters



The New Region appears in the Regions drop down list.

Figure 8-14 New Region

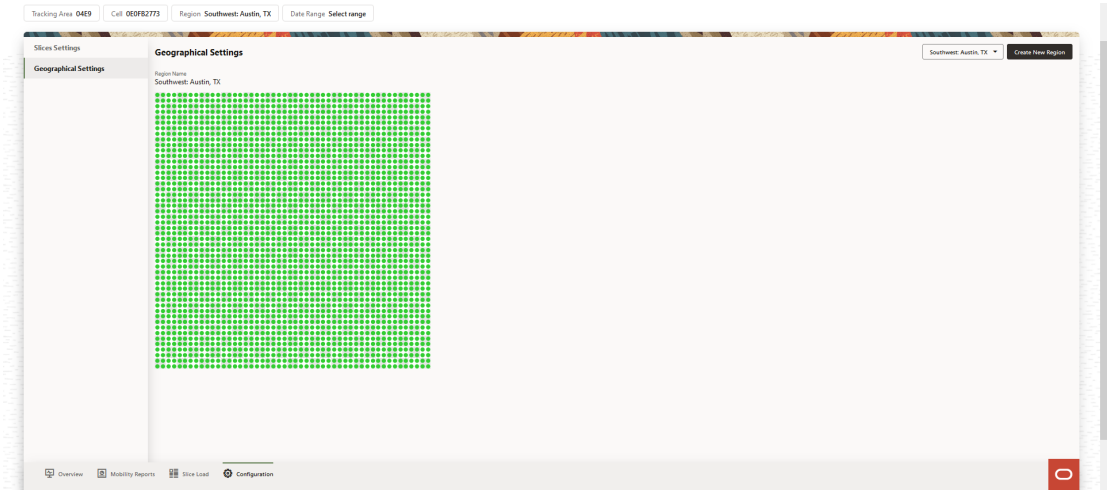


8.3.2.2 Select Existing Region and Edit Cells

The **Geographical Settings** screen has an option to **Select Existing Region**. To visualize an existing region, click **Select Existing Region** drop down and select the desired region from the displayed list.

A grid of cells in the selected region are displayed:

Figure 8-15 Existing Region



Select cell that you want to edit and the **Editing Cell** form appears on the right side of the screen:

Figure 8-16 Edit Cell

The following fields can be edited:

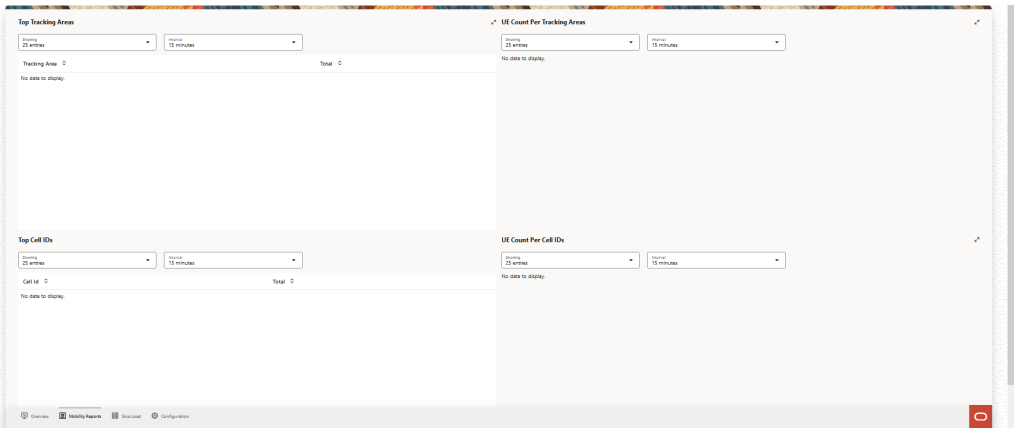
- Cell Name
- Tracking Area
- Longitude
- Latitude
- Geo Longitude
- Geo Latitude

Click **Update** to save the changes or **Cancel** to discard the changes.

8.4 Mobility Reports

After successful login, the Network Overview screen is displayed. Click the **Mobility Reports** button, and the **Mobility Reports** screen appears.

Figure 8-17 Mobility Reports



The **Mobility Reports** screen provides the following information:

- Top Tracking Areas
- UE Count Per Tracking Areas
- Top Cell IDs
- UE Count Per Cell IDs

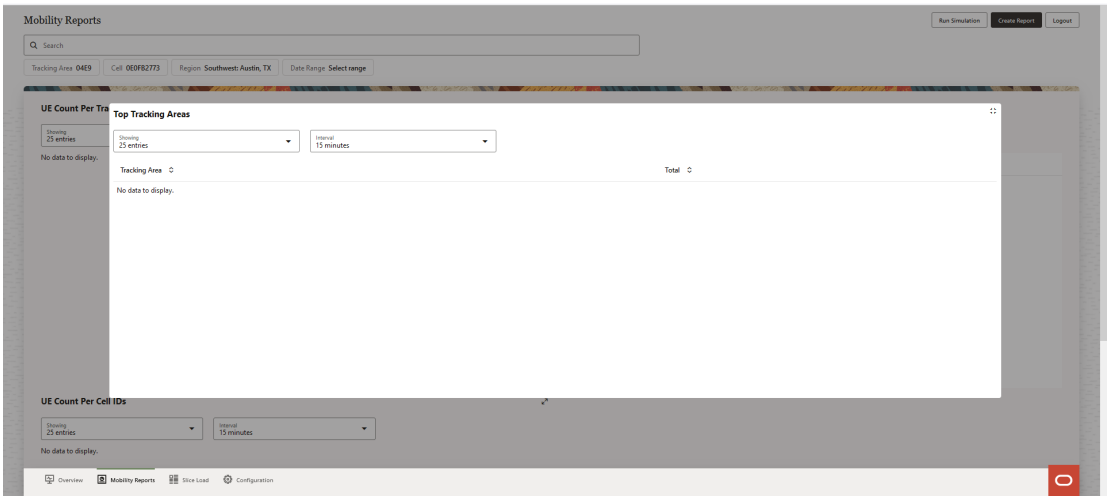
Top Tracking Areas

This section displays the **Top Tracking Areas**. Drop down options are available to select number of entries to be displayed and the time interval. Select **Showing**, to select the number of entries to be displayed, the available options are **10 entries**, **25 entries**, and **50 entries**. Select the **Interval**, the available options are **5 minutes**, **15 minutes**, **30 minutes** and **60 minutes**.

The **Tracking Area** and the **Total** are displayed based on the number of entries and interval selected in the drop down list.

User has an option to obtain an expanded view of the **Top Tracking Areas**. Click the option to expand the view, the **Top Tracking Areas** appears as a pop up on the screen.

Figure 8-18 Top Tracking Areas

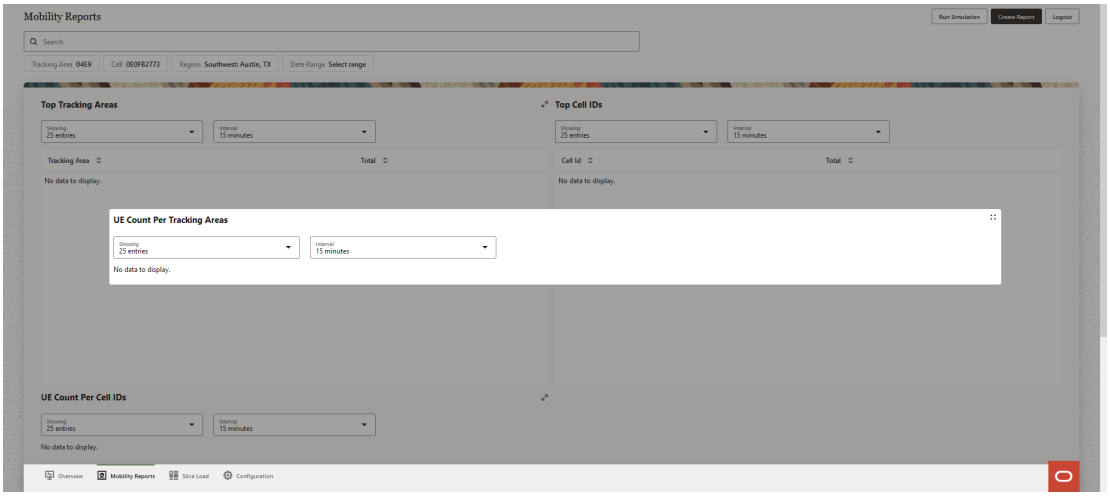


UE Count Per Tracking Areas

Displays the **UE Count Per Tracking Areas**. Drop down options are available to select number of entries to be displayed and the time interval. Select **Showing**, to select the number of entries to be displayed, the available options are **10 entries**, **25 entries**, and **50 entries**. Select the **Interval**, the available options are **5 minutes**, **15 minutes**, **30 minutes** and **60 minutes**.

User has an option to obtain an expanded view of the **UE Count Per Tracking Areas**. Click the option to expand the view, the **UE Count Per Tracking Areas** appears as a pop up on the screen.

Figure 8-19 UE Count Per Tracking Areas



Top Cell IDs

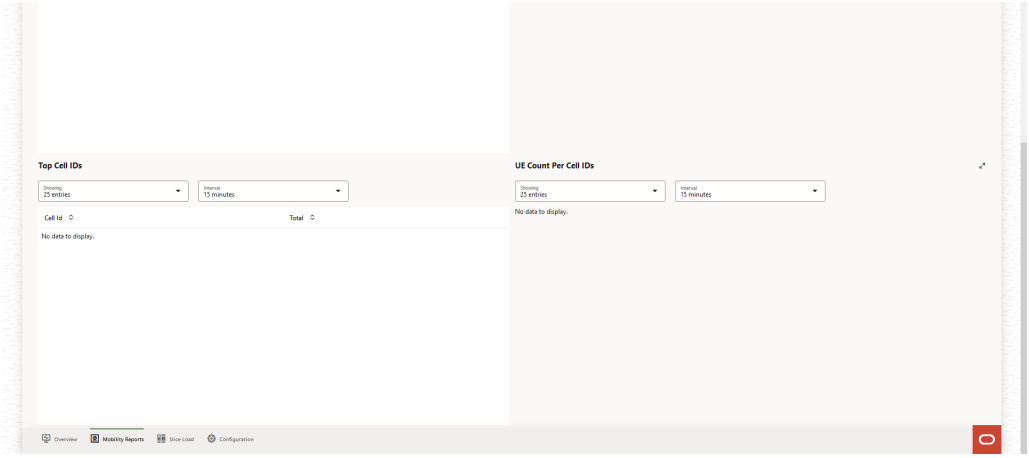
Displays the **Top Cell IDs**. Drop down options are available to select number of entries to be displayed and the time interval. Select **Showing**, to select the number of entries to be

displayed, the available options are **10 entries**, **25 entries**, and **50 entries**. Select the **Interval**, the available options are **5 minutes**, **15 minutes**, **30 minutes** and **60 minutes**.

The **Cell Id** and the **Total** are displayed based on the number of entries and interval selected in the drop down list.

User has an option to obtain an expanded view of the **Top Cell IDs**. Click the option to expand the view, the **Top Cell IDs** appears as a pop up on the screen.

Figure 8-20 Top Cell IDs

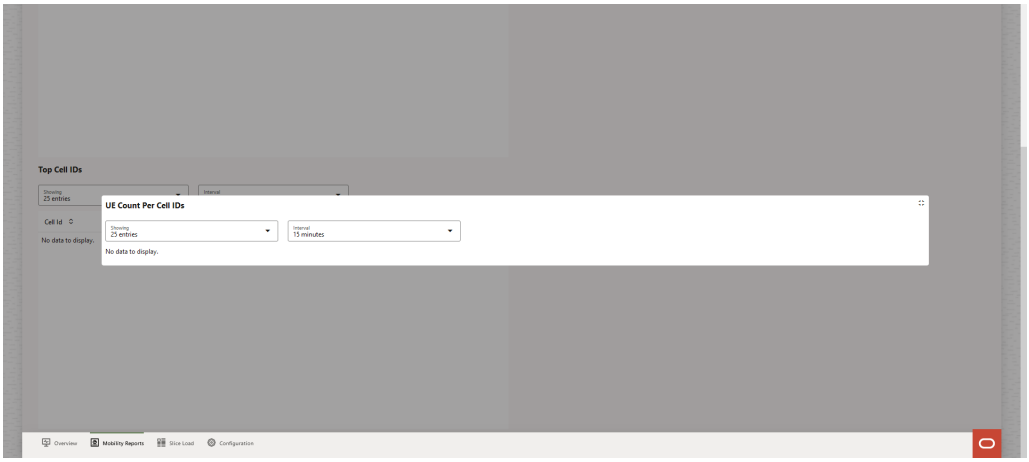


UE Count Per Cell IDs

Displays the **UE Count Per Cell IDs**. Drop down options are available to select number of entries to be displayed and the time interval. Select **Showing**, to select the number of entries to be displayed, the available options are **10 entries**, **25 entries**, and **50 entries**. Select the **Interval**, the available options are **5 minutes**, **15 minutes**, **30 minutes** and **60 minutes**.

User has an option to obtain an expanded view of the **UE Count Per Cell IDs**. Click the option to expand the view, the **UE Count Per Cell IDs** appears as a pop up on the screen.

Figure 8-21 UE Count Per Cell IDs



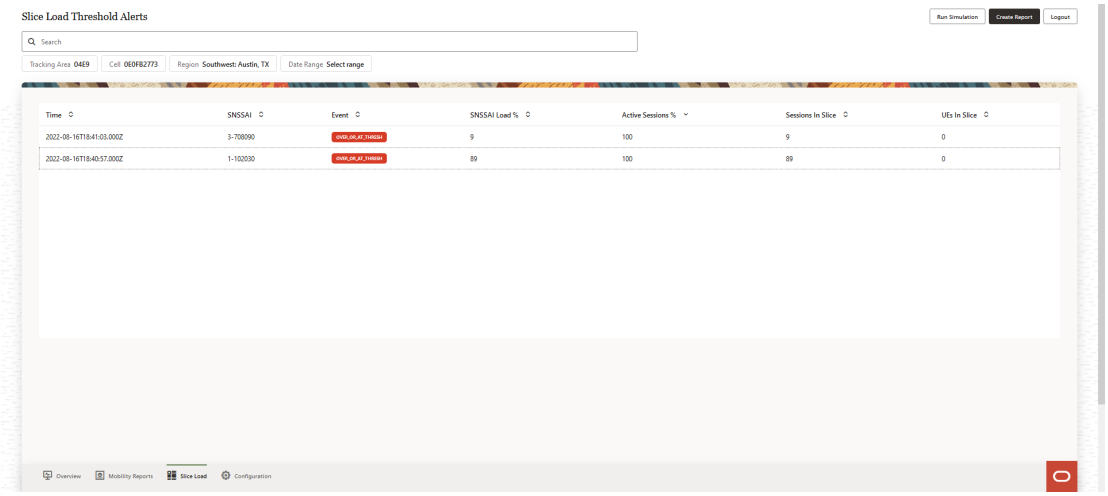
8.5 Slice Load Threshold Alerts

After successful login, the Network Overview screen is displayed. Click the **Slice Load** button, and the **Slice Load Threshold Alerts** screen appears.

The **Slice Load Threshold Alerts** displayed on the screen lists the following slice information:

- Time
- SNSSAI
- Event
- SNSSAI Load %
- Active Sessions %
- Sessions In Slice
- UEs In Slice

Figure 8-22 Slice Load Threshold Alerts



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 and UE Abnormal Behavior.

> **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.

The following APIs are invoked to obtain analytics information:

- UE Abnormal Behavior Analytics
- Slice Load Level Analytics
- UE Mobility Analytics
- NF Load 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
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	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. If this value is set to "true" the OC-NWDAF includes the reports of the events subscribed (if available), in the HTTP POST response.

Table 9-8 (Cont.) Request Body Parameters

Field Name	Data Type	Description
notifMethod	string	Event notification method. The allowed values are: • ON_EVENT_DETECTION
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" , "intGroupIds" and "anyUe" attributes.
exptAnaType	ExpectedAnalyticsType	Represents expected UE analytics type.
exptUeBehav	ExpectedUeBehaviourData	Represents expected UE behaviour.
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 "ABNORMAL_BEHAVIOUR", the following analytics are provided:

1. Identification of target UE(s) to which the subscription applies by "supis", "intGroupIds" or "anyUe" attribute in the "tgtUe" attribute.
2. Expected analytics type through the "exptAnaType" attribute.
3. Expected UE behavior through "exptUeBehav" 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 9-9 Supported Response Codes

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

Table 9-9 (Cont.) Supported Response Codes

Code	Description
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

```
{ "notificationURI": "https://{CONSUMERAPIROOT}/notification",
"supportedFeatures": "010",
"evtReq": {
        "immRep": false,
        "notifMethod": "PERIODIC",
        "maxReportNbr": 0,
        "monDur": "2022-06-24T17:00:00Z" },
"eventSubscriptions": [{
"event": "ABNORMAL_BEHAVIOUR",
"tgtUe": {
        "supis": ["{VALIDSUPID}"],
        "intGroupIds": null,
        "anyUe": false },
    "exptAnaType": "MOBILITY",
    "exptUeBehav": 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.
snssaia	String	Identifies of network slice to which the subscription belongs.

Table 9-10 (Cont.) Request Body Parameters

Field Name	Data Type	Description
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",
"snssaia": [{
    "sst": 2,
    "sd": null }] }]}
```

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 values are: • 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 • 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": "PERIODIC",
        "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.

Table 9-14 (Cont.) Request Body Parameters

Field Name	Data Type	Description
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.
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.
congThresholds	array	Represents the congestion threshold levels. • "congLevel": 20, • "nfLoadLevel": 50, • "nfCpuUsage": 90, • "nfMemoryUsage": 95, • "nfStorageUsage": 80
exptAnaType	string	It should be set to "MOBILITY" Represents expected UE analytics type. Absent if the "excepRequs" attribute is provided.

Table 9-14 (Cont.) Request Body Parameters

Field Name	Data Type	Description
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
            },
            "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"
    }
```

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,
                "nfCpuUsage": 90,
                "nfMemoryUsage": 95,
                "nfStorageUsage": 80
            }
        ],
        "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"
}
```

10
OCNWDAF Alerts

This chapter describes the following information about OCNWDAF alerts:

- OCNWDAF Alert Configuration
- System Level Alerts
- Application Level Alerts

10.1 OCNWDAF Alert Configuration

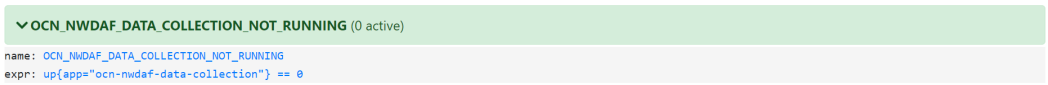
This section describes the measurement based alert rules configuration for OCNWDAF. The Alert Manager uses the Prometheus measurements values as reported by microservices in conditions under alert rules to trigger alerts.

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,p
od_template_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,p
od_template_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_temp
late_hash) (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,p
od_template_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_h
ash) (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_tem
plate_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
```

10.2 System Level Alerts

This section lists the system level alerts.

OCN_NWDAF_ANALYTICS_HIGH_CPU_LOAD

Table 10-1 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 10-2 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 10-3 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 10-4 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 10-5 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 10-6 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 10-7 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 10-8 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 the 80%.

OCN_NWDAF_COMMUNICATION_HIGH_JVM_HEAP_MEMORY_USAGE

Table 10-9 OCN_NWDAF_COMMUNICATION_HIGH_JVM_HEAP_MEMORY_USAGE

Field	Details
Description	The average of the memory heap usage is high.

Table 10-9 (Cont.) OCN_NWDAF_COMMUNICATION_HIGH_JVM_HEAP_MEMORY_USAGE

Field	Details
Affected Functions	All
Cause	The heap memory usage is more than the 80%.

OCN_NWDAF_CONFIGURATION_SERVICE_HIGH_JVM_HEAP_MEMORY_USAGE

Table 10-10 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 the 80%.

OCN_NWDAF_DATA_COLLECTION_HIGH_JVM_HEAP_MEMORY_USAGE

Table 10-11 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 the 80%.

OCN_NWDAF_GATEWAY_HIGH_JVM_HEAP_MEMORY_USAGE

Table 10-12 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 the 80%.

OCN_NWDAF_MTLF_HIGH_JVM_HEAP_MEMORY_USAGE

Table 10-13 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 the 80%.

OCN_NWDAF_SUBSCRIPTION_HIGH_JVM_HEAP_MEMORY_USAGE

Table 10-14 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 the 80%.

10.3 Application Level Alerts

This section lists the application level alerts.

OCN_NWDAF_ANALYTICS_NOT_RUNNING

Table 10-15 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 10-16 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 10-17 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 10-18 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 10-19 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 10-20 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 10-21 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 10-22 HIGH_ABNORMAL_BEHAVIOUR_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=ABNORMAL_BEHAVIOUR`

Table 10-22 (Cont.) HIGH_ABNORMAL_BEHAVIOUR_REQUEST_RATE

Field	Details
Affected Functions	ABNORMAL_BEHAVIOUR

HIGH_UE_MOBILITY_REQUEST_RATE

Table 10-23 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 10-24 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 10-25 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 10-26 HIGH_ABNORMAL_BEHAVIOUR_REQUEST_FAILURE_RATE

Field	Details
Description	The number of requests failing per second is high.

Table 10-26 (Cont.) HIGH_ABNORMAL_BEHAVIOUR_REQUEST_FAILURE_RATE

Field	Details
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 10-27 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