

Oracle® Communications

Networks Data Analytics Function Solution Guide



Release 23.1.0
F76778-01
March 2023

ORACLE®

Copyright © 2022, Oracle and/or its affiliates.

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

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

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

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

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

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

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

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

Contents

1	Introduction	
1.1	Overview	1
1.2	References	2
2	OCNWDAF Architecture	
2.1	Oracle Communications Networks Data Analytics Function Architecture	1
2.2	OCNWDAF Architecture Principles	4
3	OCNWDAF Interaction with 5G NFs and AF	
3.1	Interaction with 5G NFs	1
3.2	Interaction with Application Functions (AFs)	1
4	OCNWDAF Features	
4.1	Time Series Database	1
4.2	Support for AI Model	1
4.3	Support for ML Model and Repository	1
4.4	OCNWDAF Multicloud Strategy	2
5	OCNWDAF Analytics	
5.1	OCNWDAF Analytics	1

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	Oracle Communications Cloud Native Core, Cloud Native Environment (CNE)
CSP	Communications Service Provider
FE	Front End
FQDN	Fully Qualified Domain Name
GUI	Graphical User Interface
HTTPS	Hypertext Transfer Protocol Secure
KPI	Key Performance Indicator
HA	High Availability
IMSI	International Mobile Subscriber Identity
K8s	Kubernetes
MDT	Mobile Data Terminal
ME	Monitoring Events
MICO	Mobile Initiated Connection Only
ML	Machine Learning
MLOPs	Machine Learning Operations
MTLF	Model Training Logical Function
Network Slice	A logical network that provides specific network capabilities and network characteristics.
NEF	Oracle Communications Cloud Native Core, Network Exposure Function (NEF)
NF	Network Function
NRF	Oracle Communications Cloud Native Core, Network Repository Function (NRF)
NSI	Network Slice instance. A set of Network Function instances and the required resources (such as compute, storage and networking resources) which form a deployed Network Slice.
NSSF	Oracle Communications Cloud Native Core, Network Slice Selection Function (NSSF)
OCNWDAF	Oracle Communications Networks Data Analytics Function

Table (Cont.) Acronyms

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

What's New in This Guide

This section introduces the documentation updates for Release 23.1.0 in Oracle Communications Networks Data Analytics Function Solution Guide.

Release 23.1.0 - F76778-01, March 2023

- **NRF Client Service:** This service integrates OCNWDAF with NRF for registration, discovery, and service status or load related information, along with application and performance information services. For more information see, [Oracle Communications Networks Data Analytics Function Architecture](#) section and *Oracle Communications Networks Data Analytics Function Installation and Fault Recovery Guide*.

1

Introduction

This document provides information about the role of Oracle Communications Network Data Analytics Function (OCNWDAF) in 5G Service Based Architecture (SBA) and how to configure and use the OCNWDAF functionality and services.

1.1 Overview

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

About Oracle Communications Networks Data Analytics Function

Many Communications Service Providers (CSPs) are deploying analytics tools in their networks. However, the deployment of these tools can be complex due to their inconsistent approaches to collecting (and transmitting) data, and gathering insights on Network Functions using non-standardized proprietary interfaces. Consequently, the level of intelligence that can be gleaned from and applied back to the network and other parts of the business is limited; this impacts the pace at which CSPs can achieve their strategic objectives. With the 3rd Generation Partnership Project (3GPP) based analytics function designed to provide analytics to drive actionable insights, CSPs will have the opportunities to address the challenges.

The Oracle Communications Network Data Analytics Function (OCNWDAF) is a 3GPP defined 5G Network Function (NF) that assists in collecting and analyzing data in a 5G network. The OCNWDAF enables the CSPs 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 and producers of data are 5G NFs, AFs and OAM. The OCNWDAF broadly 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 NFs.

A 5G network contains a vast number of devices and sensors generating an enormous amount of data. The OCNWDAF function allows the 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 on past (or current) events or predictive information which can be used to balance the resources on the network. The OCNWDAF can predict the User Equipments (UEs) location and also detect if the UE is in an abnormal location. Based on the analytics information collected, the CSPs can roll out new services or modify the existing services without waiting for a network maintenance window. This ensures significantly fewer chances of the 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 consumers in the network. The OCNWDAF information can also be locally configured on the consumers. The OCNWDAF selection function in the consumers select 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 consumers that need specific analytics types query the NRF and include the Analytics ID based on its required data.

OCNWDAF is a highly scalable and agile 5G Core (5GC) network function. It not only supports the 3GPP recommended functionalities but also offers the openness in integrating with any data source (for example, data lake, common message bus, and so on), publishing analytics reports to any consumer through industry leading messaging frameworks such as Kafka. It has the potential to offer any analytics use case, including non-3GPP use cases that CSPs may require in future. OCNWDAF offers advanced deep learning capabilities such as neural networks and balancing resources versus accuracy with its two-prong ML strategy.

1.2 References

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

- *Oracle Communications Networks Data Analytics Function User Guide*
- *Oracle Communications Networks Data Analytics Function Installation and Fault Recovery Guide*
- *Oracle Communications Networks Data Analytics Function Troubleshooting Guide*
- *3GPP Technical Specification 23.288, Architecture enhancements for 5G System (5GS) to support network data analytics services*
- *3GPP Technical Specification 29.520, 5G System Network Data Analytics Services*
- *3GPP Technical Specification 29.571, 5G System Common Data Types for Service Based Interfaces*
- *3GPP Technical Specification 29.508, 5G System Session Management Event Exposure Service*
- *3GPP Technical Specification 29.518, 5G System Access and Mobility Management Services*
- *3GPP Technical Specification 33.521, 5G Security Assurance Specification (SCAS) Network Data Analytics Function (NWDAF)*
- *3GPP Technical Specification 33.926, Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes*
- *3GPP Technical Specification 33.117, Catalog of general security assurance requirements*
- *3GPP Technical Specification 23.501, System architecture for the 5G System (5GS)*
- *3GPP Technical Specification 23.502, Procedures for the 5G System (5GS)*
- *3GPP Technical Specification 28.532, Management and orchestration Generic management services*
- *3GPP Technical Specification 28.550, Management and orchestration Performance assurance*

- *3GPP Technical Specification 28.552, Management and orchestration 5G performance measurements*
- *3GPP Technical Specification 28.554, Management and orchestration 5G end to end Key Performance Indicators (KPI)*
- *3GPP Technical Specification 28.662, Telecommunication management; Generic Radio Access Network (RAN) Network Resource Model (NRM) Integration Reference Point (IRP) Information Service (IS)*
- *3GPP Technical Specification 28.623, Telecommunication management Generic Network Resource Model (NRM) Integration Reference Point (IRP) Solution Set (SS) definitions*
- *3GPP Technical Specification 32.404, Telecommunication management Performance Management (PM) Performance measurements, Definitions and template*

2

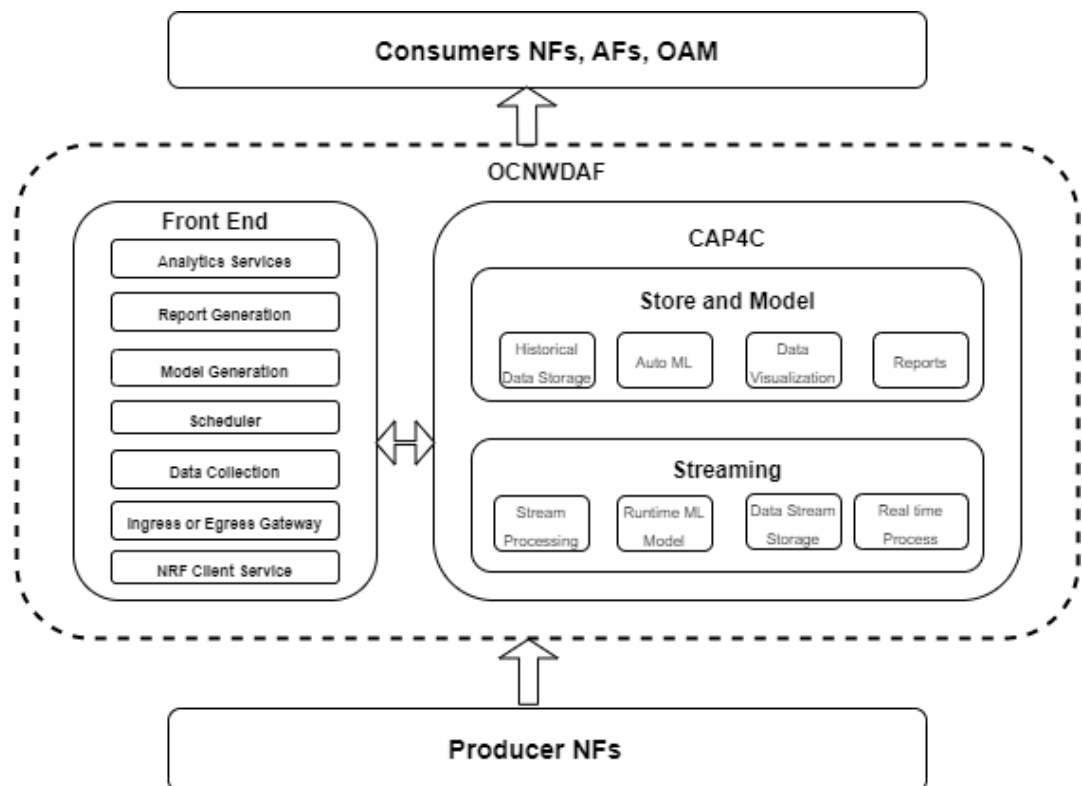
OCNWDAF Architecture

This chapter describes the Oracle Communications Network Data Analytics Function (OCNWDAF) architecture.

2.1 Oracle Communications Networks Data Analytics Function Architecture

The figure below depicts a high-level functional architecture of the OCNWDAF. The product comprises of a 3GPP gateway at the front end and an analytics platform at the backend. The 3GPP Front End (FE) is called the OCNWDAF FE, and the backend analytics platform is called the Converged Analytics Platform for Communication (CAP4C). All the Network Functions (NFs) offered by Oracle are developed based on a Cloud Native architecture. They operate in a container based Cloud Native Environment (CNE), and the OCNWDAF is no exception.

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

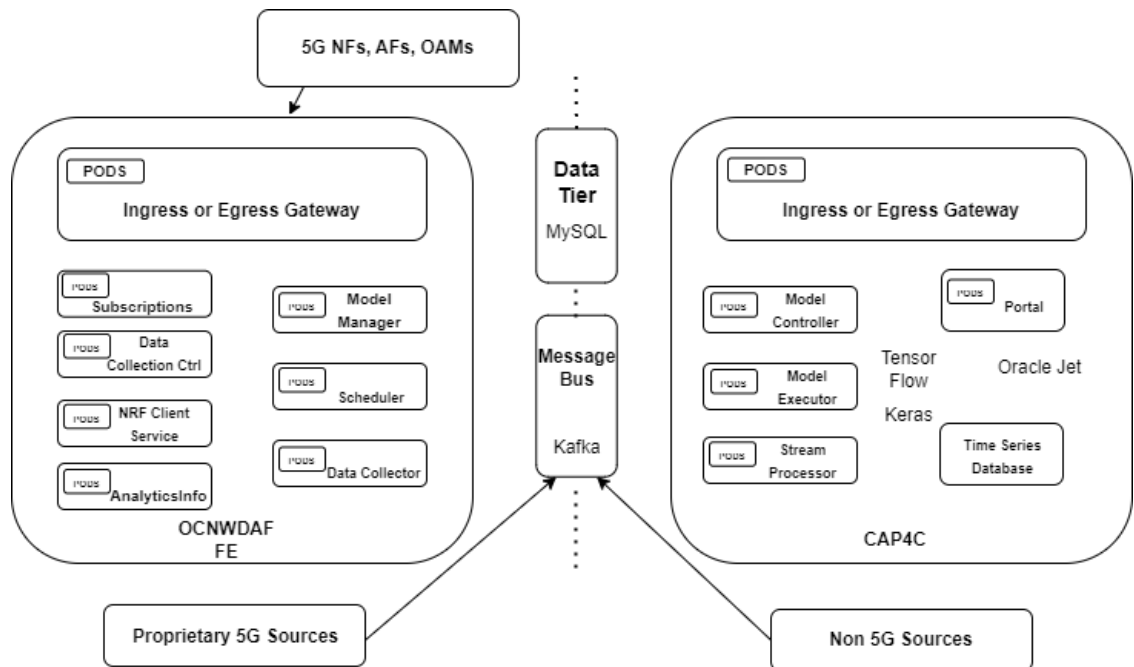
Converged Analytics Platform for Communication (CAP4C)

- 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

OCNWDAF Detailed 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.

NRF Client Service

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

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

2.2 OCNWDAF Architecture Principles

The OCNWDAF is built using Cloud Native principles. The OCNWDAF is deployed as Cloud Native Core Network Function (NF), similar to other 5G NFs. The OCNWDAF follows best practices for both the industry and customers. For example:

- OCNWDAF is based on the microservice architecture. The Front End (FE) and Converged Analytics Platform for Communication (CAP4C) are built using a set of microservices.
- The microservices are designed to perform one specific task or job.

- The microservices interact through standard interfaces (HTTP or messaging through Kafka).
- The microservices can be scaled up or down according to Kubernetes programmed rules.
- No root or elevated access is required.

Modular, Flexible, and Scalable Architecture

The flexibility of an analytics solution depends on the following factors:

- Flexibility in data collection or ingestion
- Ability to support diversified use cases
- Availability of analytics feed to the consumer (on demand, periodic, so on)

The OCNWDAF supports the above mentioned characteristics beyond what is defined in 3GPP Technical Specification for Data Analytics NFs.

- To support diversified use cases (for example, other than those defined by 3GPP), OCNWDAFs concept of separation of CAP4C from the FE provides the flexibility to support any use case category. The flexibility in creating ML models, training or retraining, model validation and benchmarking, and automated deployment make OCNWDAF the best breed.
- OCNWDAF provides the analytics report (on demand or periodic) to the consumers in different ways. For example, in the case of 3GPP network elements, the analytics report is provided through 3GPP defined (TS 23.288, TS 29.520) SBI interface.
- The OCNWDAF is evolving along the lines of 3GPP specifications and customer use case requirements. OCNWDAF is developed as an open and flexible analytics platform to meet customers' future use case requirements.
- The entire OCNWDAF functionality is modular and independent. Interactions between these entities are enabled through REST APIs, the streaming framework, the time-series database, or the DBTier. Direct messaging through REST (where synchronous communication is necessary) or messaging through Kafka (when the communication is asynchronous). Configuration data, dynamic data, and time-based data is stored by one entity and can be accessed by another for usage or display.

3

OCNWDAF Interaction with 5G NFs and AF

This chapter describes how the OCNWDAF interacts with 5G NFs and AFs in the 5G environment.

3.1 Interaction with 5G NFs

The OCNWDAF interacts with Network Functions (NFs), Application Functions (AFs), and Operations, administration and management (OAMs) through the following gateways:

- The Ingress Gateway with functions such as Ingress connection management, TLS 1.2, and OAuth2.0.
- The Egress Gateway with functions such as Egress connection management Indirect, TLS 1.2 and OAuth2.0, retry and re-route in OCNWDAF Front End (FE). Also provide a Service Based Interface (SBI) for communication with other 5G NFs.

Ingress Gateway

This will be OCNWDAF's endpoint for accessing OCNWDAF services. Ambassador Proxy can be used as an API gateway. The Ingress Gateway provides the following capabilities:

- API path routing
- Proxy Service
- Load balancing
- Circuit breaking
- Security
- Internal microservices registry

Egress Gateway

All the outgoing communication from OCNWDAF to other NFs is routed through the Egress gateway.

3.2 Interaction with Application Functions (AFs)

The OCNWDAF can provide analytics reports to Application Functions (AFs).

If the AF is external, the communication between OCNWDAF and AF is carried out through the OCNEF. As defined in 3GPP TS 29.522, OCNEF supports CAPIF (Common API Framework) to ensure the external AF communicating with OCNWDAF is trusted.

The AF can obtain the analytics report from OC-NWDAF through the services exposed by OCNWDAF (For instance, *Nnwdafl_AnalyticsInfo*).

4

OCNWDAF Features

This chapter describes OCNWDAF features.

4.1 Time Series Database

The OCNWDAF uses a time series database. The benefits of using a time series database are listed below:

- The database searches faster as it is organized based on time and not any other key values. It can ingest millions of records, store trillions, and maintain query latencies from a sub-second level in just a few seconds. Unlike any public cloud data warehouse, database query latency is at least three times faster.
- Purging the older data is much cheaper than relational databases. Information is stored based on time in segments. An entire time segment can be quickly and easily cleared, or even dropped from the cluster but not from deep storage, still available at a higher latency for some rare access scenarios.
- Another significant benefit of using this database is data roll-up. The database can roll the data into 15-minute, 1-hour, and daily entries. The database can be designed in such a manner that the minor entries can start ageing out in a few months and the 15-minute entries can start ageing out in six months. After a year, the 1-hour entries can age out. This functionality significantly reduces the amount of data that has to be stored but still provides scope for extensive historical data.

4.2 Support for AI Model

The OCNWDAF supports the industry's best ML frameworks, such as TensorFlow and scikit-learn. Many supported models, including Neural Networks and specialized versions such as Long Short Term Memory, are used.

4.3 Support for ML Model and Repository

The main constraints of machine learning models are the time necessary to train the model and the accuracy observed from the model. We are focusing on a two-prong approach described below to ensure both the constraints are minimized:

- The ML models will be developed for the use cases and analytics categories will be used in a very general and broad manner. This further ensures:
 - The ML models can automatically self-optimize by using the industry's best hyper-parameter optimization algorithms.

All ML model storage will be in the ONNX format, along with an analytics type, model version, data version (define the scope of data used), and timestamp. Any external model support added should be in ONNX format.

4.4 OCNWDAF Multicloud Strategy

Oracle is a platinum member of the Cloud Native Computing Foundation (CNCf) and aligns with the CNCf's vision of an open, cloud-native, and standard approach to develop applications. Based in-depth understanding of service reliability, Oracle strives to create foundational platform services where applications are built to provide service reliability.

Oracle's OCNWDAF and Cloud Native Environment (OC-CNE) are based on industries leading open-source services and tools, this enable operations and management of OCNWDAF in a production-grade environment. Oracle has adopted software architecture principles to support Communications Service Providers multicloud strategy.

- The Cloud Native Framework represents a collection of shared services which OC-NWDAF uses. Oracle maintains a reference Cloud Native Framework utilising a selection of open-source components and tools for development. The deployment CNE must provide all the Cloud Native Framework services but is free to select the specific version and component providing the service. For example, Oracle's OC-NWDAF supports operation with CSPs' version of Prometheus and can support either Jaeger or Zipkin for distributed tracing. A DevOps CI/CD model is supported to ensure OC-NWDAF is thoroughly tested and is fully operational in the deployment environment.
- Kubernetes' environment provides runtime and lifecycle management services. Like the Cloud Native Framework, Oracle maintains a reference Kubernetes environment but allows CSPs to select the specific version used in the deployment CNE. OC-NWDAF runs in a containerized environment, uses Kubernetes DNS for service discovery, and can support a variety of Container Network Interfaces which integrate Oracle NFs networking requirements with the deployment SDN environment. The services lifecycle is controlled, deployment specific configuration is permitted and environment files are dynamically associated with the OC-NWDAF. Helm charts are used for packaging the component microservices into the OC-NWDAF applications. The configured repository handles the versioning available for each service and component microservices. Operators can enable Kubernetes deployments to manage the lifecycle of the OC-NWDAF, including the initial roll-out of the service, roll-out of a canary release to validate a new version, and roll-out of an upgrade to a new version.
- Oracle continuously delivers new functionality into the Oracle Portal. Customers are notified and may choose to trigger their CI/CD workflow to deploy the new functionality. Oracle's Communications Global Business Unit implements and executes automated unit tests for each component and service as part of the build process. Automated integration tests are run using the reference Cloud Native Framework to ensure that each component's runtime services and exposed APIs operate as expected. Other automated integration tests ensure APIs and NF components are functional and the overall business logic of the NF is operational. Oracle CGBU includes the subset of these test artefacts (which validate operation with the runtime environment and Cloud Native Framework) with the images of the NF components. Customers can incorporate these automated tests in the target deployment environment.
- Oracle Communications Automated Test Tools and Scripts (ATS) helps operators to automate the complete testing lifecycle of 5G NFs. This aids in accelerating innovation as software delivery times are significantly shortened. There is a considerable benefit in deploying an automated testing solution in terms of cost, effort, and overall test coverage. With the adoption of DevOps and CI/CD in the Telecommunication domain, number of software releases has significantly increased thus making manual testing very challenging. Oracle Communications ATS helps operators to execute functional, regression and performance test cases easily without user intervention. As a result, operators can quickly deploy new software releases and rapidly roll out new features.

5

OCNWDAF Analytics

This chapter describes the OCNWDAF analytics information.

5.1 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 OCNWDAF provides the following analytics information:

- Slice Load level information
- UE mobility information
- UE Abnormal behaviour information (unexpected UE location)
- NF Load Level Analytics