Oracle® Communications

Network Analytics Data Director Release Notes

Release 22.0.0
F72106-03
January 2023

ORACLE

Oracle Communications Network Analytics Data Director Release Notes, Release 22.0.0

F72106-03

Contents

My Oracle Support (MOS)

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

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

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

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

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

What's New in This Guide

This section lists the documentation updates for Release *22.0.0* in *Oracle Communications Network Analytics Data Director Release Notes*.

Release 22.0.0 - F72106-03, January 2022

Updated the document with editorial changes.

Release 22.0.0 - F72106-02, December 2022

Updated the document with cosmetic changes.

Release 22.0.0 - F72106-01, December 2022

This is the first release of the document.

1 Introduction

This document provides information about features of Oracle Communications Network Analytics Data Director (OCNADD).

It also includes details related to media pack, common services, security certification declaration, and documentation pack. The detailed information of the fixes are included in the Resolved Bug List section. For issues that are not yet addressed, see the Customer Known Bug List.

For information on how to access key Oracle sites and services, see My Oracle Support (MOS).

2
Feature Descriptions

This chapter provides a summary of the features for Oracle Communications Network Analytics Data Director (OCNADD) release 22.0.0.

OCNADD release 22.0.0 provides the following features:

- **Helm-based Installation**: OCNADD supports helm-based installation on the OCCNE and TANZU platforms through a clear sequence of procedures. For information on OCNADD installation and uninstallation procedures, see *Oracle Communications Network Analytics Data Director Installation Guide*.
- **Data Aggregation**: OCNADD collects and aggregates network traffic from multiple NFs (for example, SCP 1 & 2 and SEPP, and NRF) and provides the aggregated traffic feed to one or many third-party monitoring tools. The aggregation rules can be configured during the third-party application configuration using OCNADD GUI. For more information on data aggregation, see *Oracle Communications Network Analytics Data Director User Guide*.
- **Secure Transport**: OCNADD provides secure data communication between producer NFs and third-party consumer applications. The incoming data streaming towards OCNADD and outgoing data streaming towards third-party applications are TLS encrypted. The TLS can be disabled and enabled for the third-party applications using the configuration feature via OCNADD GUI. For more information, see *Oracle Communications Network Analytics Data Director User Guide*.
- **Graphical User Interface**: OCNADD provides a rich set of insights in the form of operational dashboards that provide visualization for various metrics, KPIs, and alarms. Also, OCNADD provides an intuitive and simple workflow-based GUI to configure the third-party application feed. For more information on OCNADD GUI, see *Oracle Communications Network Analytics Data Director User Guide*.
- **Health monitoring**: OCNADD monitors readiness and liveliness of each service with its instances and provides an immediate alert about any malfunction. For example, MAX number of replica for service has been instantiated, Particular service is in down state, or Max number of CPU/MEMORY threshold has been reached. OCNADD also provides a health report of each service, which can be requested on demand or periodically in the OCNADD dashboard. For more information, see *Oracle Communications Network Analytics Data Director User Guide*.
- **High Availability**: OCNADD supports microservice based architecture and OCNADD instances are deployed in Cloud Native Environments (CNEs) that ensures high availability of services and auto scaling based on resource utilization. For more information, see *Oracle Communications Network Analytics Data Director User Guide*.
- **Metrics, KPIs, and Alerts**: OCNADD provides a rich set of metrics, KPIs, and threshold alerts that are integrated with the Prometheus. A few critical KPIs are also integrated with the operational dashboard provided by the OCNADD GUI service. A few of the important KPIs and Alerts are Ingress MPS, Egress MPS, Latency between producer NF and OCNADD, and Failure Alerts. For more information, see *Oracle Communications Network Analytics Data Director User Guide*.
- **Backup and Restore**: OCNADD provides backup and restore procedures for disaster recovery. Operators can take an OCNADD site or a namespace specific database and

required Kubernetes resources for backup to restore on the same or a different Kubernetes cluster. The backup and restore procedures are helpful in disaster recovery, cluster migration, setup replication from production to development or staging, and cluster upgrade to new OCCNE version or Kubernetes version. For more information, see *Oracle Communications Network Analytics Data Director Backup and Disaster Recovery Guide*.

3
Media and Documentation

Media Pack

This section lists the media package for Oracle Communications Network Analytics Data Director (OCNADD) 22.0.0. To download the media package, see My Oracle Support (MOS).

> **Note:**
>
> The information provided in this section is accurate at the time of release but is subject to change. See the Oracle software delivery website for the latest information.

Table 3-1 Media Pack Contents for OCNADD 22.0.0

Description	NF Version	ATS Version	Upgrade Supported
Oracle Communications Network Analytics Data Director (OCNADD)	22.0.0	22.4.0	OCNADD 22.0.0 supports fresh installation and upgrade from 22.0.x. The upgrade does not include the schema changes for the first release of OCNADD. For more information on installation or upgrade, see *Oracle Communications Network Analytics Installation*.

Compliance Matrix

The following table lists the compliance matrix for OCNADD:

Table 3-2 Compliance Matrix

OCCNE	DBTier	CDCS	OSO	Kubernetes	CNC Console	SCP	NRF	3GPP
22.3.x	22.3.x	NA	NA	1.23.x	22.4.x	22.4.x	22.4.x	OCNADD: NA SCP: Release 16 compliant NRF: Release 16 compliant

Note:

For the data being sent from NRF, GZIP compression is turned off within the NRF.

Note:

For the data being sent from SCP, OCNADD copies the base64 encoded compressed “5g-sbi- message” to the 3rd party consumer without decoding.

Security Certification Declaration

The following table lists the security tests and the corresponding dates of compliance for OCNADD:

Table 3-3 Security Certification Declaration

System test on functional and security features	Regression testing on security configuration	Vulnerability testing	Fuzz testing on external interfaces
17th November 2022	17th November 2022	17th November 2022	17th November 2022

Documentation Pack

All documents for OCNADD 22.0.0 available for download from the Oracle Help Center (OHC) and MOS.

4
Resolved and Known Bugs

This chapter lists the resolved and known bugs for Oracle Communications Network Analytics Data Director (OCNADD) Release 22.0.0 .

These lists are distributed to customers with a new software release at the time of General Availability (GA) and are updated for each maintenance release.

Severity Definitions

Resolved Bug List

Known Bug List

Severity Definitions

Service requests for supported Oracle programs may be submitted by you online through Oracle's web-based customer support systems or by telephone. The service request severity level is selected by you and Oracle and should be based on the severity definitions specified below.

Severity 1

Your production use of the supported programs is stopped or so severely impacted that you cannot reasonably continue work. You experience a complete loss of service. The operation is mission critical to the business and the situation is an emergency. A Severity 1 service request has one or more of the following characteristics:

- Data corrupted.
- A critical documented function is not available.
- System hangs indefinitely, causing unacceptable or indefinite delays for resources or response.
- System crashes, and crashes repeatedly after restart attempts.

Reasonable efforts will be made to respond to Severity 1 service requests within one hour. For response efforts associated with Oracle Communications Network Software Premier Support and Oracle Communications Network Software Support & Sustaining Support, please see the Oracle Communications Network Premier & Sustaining Support and Oracle Communications Network Software Support & Sustaining Support sections above.

Except as otherwise specified, Oracle provides 24 hour support for Severity 1 service requests for supported programs (OSS will work 24x7 until the issue is resolved) when you remain actively engaged with OSS working toward resolution of your Severity 1 service request. You must provide OSS with a contact during this 24x7 period, either on site or by phone, to assist with data gathering, testing, and applying fixes. You are requested to propose this severity classification with great care, so that valid Severity 1 situations obtain the necessary resource allocation from Oracle.

Severity 2

You experience a severe loss of service. Important features are unavailable with no acceptable workaround; however, operations can continue in a restricted fashion.

Severity 3

You experience a minor loss of service. The impact is an inconvenience, which may require a workaround to restore functionality.

Severity 4

You request information, an enhancement, or documentation clarification regarding your software but there is no impact on the operation of the software. You experience no loss of service. The result does not impede the operation of a system.

Resolved Bug List

There are no resolved bugs in this release.

Known Bug List

The following table lists the known bugs for OCNADD Release 22.0.0.

Table 4-1 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
34786365	OCNADD logs Error logs as INFO for Configuration service when it is sending Notification to Adapter	The logs are printed as INFO instead of ERROR in this scenario.	No system impact	3	22.0.0
34770614	EGW instances keep increasing on every re-start	De-registration does not happen when a POD gets restarted.	No system impact	3	22.0.0
34740421	OCNADD logging Error logs as INFO for Adapter and EGW when 3rd Party consumer is not reachable or is down	The logs are being printed as INFO instead of ERROR in this particular scenario.	No system impact	3	22.0.0

Table 4-1 (Cont.) Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
34740391	OCNADD GUI not validating endpoints	The URI endpoints for third-party consumer application is not getting validated. For example, extra spaces and HTTPs is used in case of No-TLS.	Missing validation can result in an incorrect configuration, however, there is no impact when the correct information is provided during the configurations .	3	22.0.0
34716751	Heart Beat logs are not showing up (verified on Alarm Service)	The heartbeat logs are printed only in Debug mode.	No system impact	3	22.0.0
34714292	Performance Execution: Gateway POD has restarted with IllegalReferenceCountException exception during 39K MPS	When there are frequent errors reported from a third-party application at high traffic rate, then these "IllegalReferenceCountException" exceptions could occur, due to which there may be EGW pod restart.	If any EGW POD goes out of memory, then liveliness checks will re-spawn the new pod instantly, and the user may get an alert of POD restart, however, there will not be any message loss.	3	22.0.0
34712921	The x-axis is not giving correct interval	In the dashboard section of GUI, the Bar graph does not display correct intervals on the x-axis, it shows multiple zeros and ones.	The user is not be able to see the correct x-axis values.	3	22.0.0

Table 4-1 (Cont.) Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
34793856	Alarms reporting such as Max replica crossed 90% for a service such as adminservice when replica is 1	The alarm "Max Replica crossed 90% for a service" is raised even though the replica count is one. The alarm should not be raised for services that do not require more than one replica count.	No system impact.	4	22.0.0
34785610	Connection status not changing to Inactive in GUI	The connection status does not change back to an Inactive state, even when directed to the random(wrong) endpoint of a third-party application.	When the configured endpoint is not valid, the incorrect connection status of the third-party feed is shown, however, there is no impact when the correct information is provided during the configurations.	4	22.0.0

Table 4-1 (Cont.) Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
34742422	Use OPTIONS request in Retry Mechanism of Adapter	Consumer Adapter's Retry Mechanism needs to update to use HTTP OPTIONS method instead of the existing implementation of periodic retrying with few messages. This scenario is observed only when the circuit breaker is enabled in OCNADD. The retry mechanism sends a message periodically to check the status of the endpoints, this will continue until the endpoint status is up and running.	Few of the messages will be delivered again to the endpoint, however, there will not be any data loss in this scenario.	4	22.0.0
34684038	Not able to change logging type to JSON	The logs are not printed in JSON format.	Users are able to see all the information in plain text format but not in JSON format.	4	22.0.0