Oracle® Communications

Cloud Native Core Release Notes

Release 2.23.1
F78388-40
September 2024

Oracle Communications Cloud Native Core Release Notes, Release 2.23.1

F78388-40

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.

What's New In This Guide

Release 2.23.1 - F78388-40, September 2024

Added a note regarding the "Updating OpenStack Credentials" procedure update in the Cloud Native Environment (CNE) section.

Release 2.23.1 - F78388-39, January 2024

CNE 23.1.4 Release

Updated the following sections with the details of CNE release 23.1.4:

- Media Pack
- Compatibility Matrix
- CNE Resolved Bugs

Release 2.23.1 - F78388-38, October 2023

Policy 23.1.8 Release

Updated the following sections with the details of Policy release 23.1.8:

- Media Pack
- Compatibility Matrix
- Common Microservices Load Lineup
- Security Certification Declaration
- Policy Known Bugs

BSF 23.1.4 Release

Updated the following sections with the details of BSF release 23.1.4:

- Media Pack
- Compatibility Matrix
- Common Microservices Load Lineup
- Security Certification Declaration

Release 2.23.1 - F78388-37, October 2023

UDR 23.1.3 Release

Updated the following sections with the details of UDR release 23.1.3:

- Media Pack
- Compatibility Matrix
- Common Microservices Load Lineup
- Security Certification Declaration
- UDR Resolved Bugs

Release 2.23.1 - F78388-36, October 2023

CNE 23.1.3 Release

Updated the following sections with the details of CNE release 23.1.3:

- Cloud Native Environment (CNE)
- Media Pack
- Compatibility Matrix
- CNE Resolved Bugs

NEF 23.1.4 Release

Updated the following sections with the details of NEF release 23.1.4:

- Media Pack
- Compatibility Matrix
- Common Microservices Load Lineup
- Security Certification Declaration
- NEF Resolved Bugs

NRF 23.1.4 Release

Updated the following sections with the details of NRF release 23.1.4:

- Media Pack
- Compatibility Matrix
- Common Microservices Load Lineup
- Security Certification Declaration

SEPP 23.1.4 Release

Updated the following sections with the details of SEPP release 23.1.4:

- Media Pack
- Compatibility Matrix
- Common Microservices Load Lineup
- Security Certification Declaration
- SEPP Resolved Bugs

Release 2.23.1 - F78388-35, October 2023

CNC Console 23.1.3 Release

Updated the following sections with details of CNC Console release 23.1.3:

- Media Pack
- Compatibility Matrix
- Common Microservices Load Lineup
- Security Certification Declaration
- CNC Console Resolved Bugs

- CNC Console Known Bugs

Release 2.23.1 - F78388-34, October 2023

cnDBTier 23.1.0, 23.1.1, 23.1.2, and 23.1.3 Releases

Added bugs for cnDBTier release 23.1.0, 23.1.1, 23.1.2, and 23.1.3 in the cnDBTier Known Bugs section.

Release 2.23.1 - F78388-33, September 2023

cnDBTier 23.1.3 Release

Updated the following sections with the details of cnDBTier release 23.1.3:

- Media Pack
- Compatibility Matrix
- cnDBTier Resolved Bugs

Release 2.23.1 - F78388-32, September 2023

cnDBTier 23.1.1 and 23.1.2 Releases

Added bugs for cnDBTier release 23.1.1 and 23.1.2 in the cnDBTier Known Bugs section.

Release 2.23.1 - F78388-31, September 2023

NRF 23.1.3 Release

Updated the following sections with the details of NRF release 23.1.3:

- Media Pack
- Compatibility Matrix
- Common Microservices Load Lineup
- Security Certification Declaration
- NRF Resolved Bugs

Release 2.23.1 - F78388-30, September 2023

CDCS 23.1.1 Release

Updated the Compatibility Matrix section with the CNE compatible versions.

CDCS 23.1.0 Release

Updated the Compatibility Matrix section with the CNE compatible versions.

Release 2.23.1 - F78388-29, August 2023

Policy 23.1.7 Release

Updated the following sections with the details of Policy release 23.1.7:

- Media Pack
- Compatibility Matrix
- Common Microservices Load Lineup
- Security Certification Declaration

- Policy Resolved Bugs
- Policy Known Bugs

Release 2.23.1 - F78388-28, August 2023

BSF 23.1.3 Release

Updated BSF Resolved Bugs section with bug details.

Release 2.23.1 - F78388-27, August 2023

BSF 23.1.3 Release

Updated the following sections with the details of BSF release 23.1.3:

- Media Pack
- Compatibility Matrix
- Common Microservices Load Lineup
- Security Certification Declaration

cnDBTier 23.1.2 Release

Added a bug in the cnDBTier Known Bugs section.

Release 2.23.1 - F78388-26, July 2023

CNC Console 23.1.2 Release

Updated the following sections with the details of CNC Console release 23.1.2:

- Media Pack
- Compatibility Matrix
- Common Microservices Load Lineup
- Security Certification Declaration
- CNC Console Resolved Bugs

NEF 23.1.3 Release

Updated the following sections with the details of NEF release 23.1.3:

- Media Pack
- Compatibility Matrix
- Common Microservices Load Lineup
- Security Certification Declaration

NRF 23.1.2 Release

Updated the following sections with the details of NRF release 23.1.2:

- Media Pack
- Compatibility Matrix
- Common Microservices Load Lineup
- Security Certification Declaration
- NRF Resolved Bugs

NSSF 23.1.2 Release

Updated the following sections with the details of NSSF release 23.1.2:

- Media Pack
- Compatibility Matrix
- Common Microservices Load Lineup
- Security Certification Declaration
- NSSF Resolved Bugs
- NSSF Known Bugs

UDR 23.1.2 Release

Updated the following sections with the details of UDR release 23.1.2:

- Media Pack
- Compatibility Matrix
- Common Microservices Load Lineup
- Security Certification Declaration
- UDR Resolved Bugs

Release 2.23.1 - F78388-25, July 2023

SEPP 23.1.3 Release

Updated the following sections with the details of SEPP release 23.1.3:

- Media Pack
- Compatibility Matrix
- Common Microservices Load Lineup
- Security Certification Declaration
- SEPP Resolved Bugs

Release 2.23.1 - F78388-24, July 2023

SCP 23.1.3 Release

Updated the following sections with the details of SCP release 23.1.3:

- Media Pack
- Compatibility Matrix
- Common Microservices Load Lineup
- Security Certification Declaration
- SCP Resolved Bugs
- SCP Known Bugs

cnDBTier 23.1.2 Release

Added a new bug in the cnDBTier Resolved Bugs section.

Release 2.23.1 - F78388-23, July 2023

cnDBTier 23.1.2 Release

Updated the following sections with the details of cnDBTier release 23.1.2:

- Media Pack
- Compatibility Matrix
- cnDBTier Resolved Bugs
- cnDBTier Known Bugs

CNE 23.1.2 Release

Updated the following sections with the details of CNE release 23.1.2:

- Media Pack
- Compatibility Matrix
- CNE Resolved Bugs
- CNE Known Bugs

Release 2.23.1 - F78388-22, July 2023

Policy 23.1.6 Release

Updated the following sections with the details of Policy release 23.1.6:

- Media Pack
- Compatibility Matrix
- Common Microservices Load Lineup
- Security Certification Declaration
- Policy Resolved Bugs
- Policy Known Bugs

BSF 23.1.2 Release

Updated the following sections with the details of BSF release 23.1.2:

- Media Pack
- Compatibility Matrix
- Common Microservices Load Lineup
- Security Certification Declaration
- BSF Resolved Bugs
- BSF Known Bugs

Release 2.23.1 - F78388-21, June 2023

Made formatting changes.

Release 2.23.1 - F78388-20, June 2023

SEPP 23.1.2 Release

Updated the following sections with the details of SEPP release 23.1.2:

- Media Pack
- Compatibility Matrix
- Common Microservices Load Lineup
- Security Certification Declaration
- SEPP Resolved Bugs
- SEPP Known Bugs

Release 2.23.1 - F78388-19, May 2023

Policy 23.1.5 Release

Updated the following sections with the details of Policy release 23.1.5:

- Media Pack
- Compatibility Matrix
- Common Microservices Load Lineup
- Security Certification Declaration
- Policy Resolved Bugs
- Policy Known Bugs

Release 2.23.1 - F78388-18, May 2023

Policy 23.1.4 Release

Updated the following sections with the details of Policy release 23.1.4:

- Media Pack
- Compatibility Matrix
- Common Microservices Load Lineup
- Security Certification Declaration
- Policy Resolved Bugs
- Policy Known Bugs

Release 2.23.1 - F78388-17, May 2023

SCP 23.1.2 Release

Updated the following sections with the details of SCP release 23.1.2:

- Media Pack
- Compatibility Matrix
- Common Microservices Load Lineup
- Security Certification Declaration
- SCP Resolved Bugs
- SCP Known Bugs

Release 2.23.1 - F78388-16, May 2023

CNC Console 23.1.1 Release

Updated the title of resolved bug 35154799 in CNC Console Resolved Bugs section for CNC Console release 23.1.1.

Release 2.23.1 - F78388-15, May 2023

SEPP ATS 23.1.2 Release
Updated the SEPP Known Bugs section for SEPP ATS release 23.1.2.

Release 2.23.1 - F78388-14, April 2023

NEF 23.1.2 Release:

Updated the following sections with the details of NEF release 23.1.2:

- Media Pack
- Compatibility Matrix
- Common Microservices Load Lineup
- Security Certification Declaration
- NEF Resolved Bugs

Policy 23.1.3 Release

Updated the following sections with the details of Policy release 23.1.3:

- Media Pack
- Compatibility Matrix
- Common Microservices Load Lineup
- Security Certification Declaration
- Policy Resolved Bugs
- Policy Known Bugs

Release 2.23.1 - F78388-13, April 2023

cnDBTier 23.1.1 Release:

Updated the following sections with the details of cnDBTier release 23.1.1:

- Cloud Native Core cnDBTier
- cnDBTier Resolved Bugs
- cnDBTier Known Bugs

CNE 23.1.1 Release:

Updated the following sections with the details of CNE release 23.1.1:

- Cloud Native Environment (CNE)
- CNE Known Bugs

CNE 23.1.0 Release:

Updated the following sections with the details of CNE release 23.1.0:

- CNE Known Bugs

Release 2.23.1 - F78388-12, April 2023

SEPP ATS 23.1.2 Release

Updated the SEPP Resolved Bugs section for SEPP ATS release 23.1.2.

Release 2.23.1 - F78388-11, April 2023

Policy 23.1.2 Release

Updated the following sections with the details of Policy release 23.1.2:

- Media Pack
- Compatibility Matrix
- Common Microservices Load Lineup
- Security Certification Declaration
- Policy Resolved Bugs
- Policy Known Bugs

BSF 23.1.1 Release

Updated the following sections with the details of BSF release 23.1.1:

- Media Pack
- Compatibility Matrix
- Common Microservices Load Lineup
- Security Certification Declaration
- BSF Resolved Bugs
- BSF Known Bugs

Release 2.23.1 - F78388-09, April 2023

SCP 23.1.1 Release

Updated the following sections with the details of SCP release 23.1.1:

- Media Pack
- Compatibility Matrix
- Common Microservices Load Lineup
- Security Certification Declaration
- SCP Resolved Bugs
- SCP Known Bugs

CDCS 23.1.1 Release

Updated the following sections with the details of CDCS release 23.1.1:

- Continuous Delivery Control Server (CDCS)
- Media Pack
- Compatibility Matrix

- CDCS Resolved Bugs

Release 2.23.1 - F78388-08, April 2023

CNE 23.1.1 Release

Updated the following sections with the details of CNE release 23.1.1:

- Media Pack
- Compatibility Matrix
- CNE Resolved Bugs
- CNE Known Bugs

CNC Console 23.1.1 Release

Updated the following sections with the details of CNC Console release 23.1.1:

- Media Pack
- Compatibility Matrix
- Common Microservices Load Lineup
- Security Certification Declaration
- CNC Console Resolved Bugs

NEF 23.1.1 Release

Updated the following sections with the details of NEF release 23.1.1:

- Media Pack
- Compatibility Matrix
- Common Microservices Load Lineup
- Security Certification Declaration
- NEF Resolved Bugs

NRF 23.1.1 Release

Updated the following sections with the details of NRF release 23.1.1:

- Network Repository Function (NRF)
- Media Pack
- Compatibility Matrix
- Common Microservices Load Lineup
- Security Certification Declaration
- NRF Resolved Bugs

NSSF 23.1.1 Release

Updated the following sections with the details of NSSF release 23.1.1:

- Network Slice Selection Function (NSSF)
- Media Pack
- Compatibility Matrix
- Common Microservices Load Lineup

- Security Certification Declaration
- NSSF Resolved Bugs
- NSSF Known Bugs

SEPP 23.1.1 Release

Updated the following sections with the details of SEPP release 23.1.1:

- Media Pack
- Compatibility Matrix
- Common Microservices Load Lineup
- Security Certification Declaration
- SEPP Resolved Bugs

UDR 23.1.1 Release

Updated the following sections with the details of UDR release 23.1.1:

- Media Pack
- Compatibility Matrix
- Common Microservices Load Lineup
- Security Certification Declaration
- UDR Resolved Bugs

Release 2.23.1 - F78388-07, April 2023

cnDBTier 23.1.1 Release

Updated the following sections with the details of cnDBTier release 23.1.1:

- Cloud Native Core cnDBTier
- Media Pack
- Compatibility Matrix
- cnDBTier Resolved Bugs

Release 2.23.1 - F78388-06, March 2023

cnDBTier 23.1.0 Release

Updated the following sections with the details of cnDBTier release 23.1.0:

- Cloud Native Core cnDBTier
- cnDBTier Known Bugs

Release 2.23.1 - F78388-05, March 2023

Policy 23.1.1 Release

Updated the following sections with the details of Policy release 23.1.1:

- Media Pack
- Compatibility Matrix
- Common Microservices Load Lineup

- Security Certification Declaration
- Policy Resolved Bugs
- Policy Known Bugs

Release 2.23.1 - F78388-04, March 2023

CNE 23.1.0 Release

Updated the following sections with the details of CNE release 23.1.0:

- Cloud Native Environment (CNE)
- Media Pack
- Compatibility Matrix
- CNE Resolved Bugs
- CNE Known Bugs

Release 2.23.1 - F78388-03, March 2023

NSSF 23.1.0 Release

Updated the following sections with the details of NSSF release 23.1.0:

- Network Slice Selection Function (NSSF)
- Media Pack
- Compatibility Matrix
- Common Microservices Load Lineup
- Security Certification Declaration
- NSSF Resolved Bugs
- NSSF Known Bugs

UDR 23.1.0 Release

Updated the following sections with the details of UDR release 23.1.0:

- Unified Data Repository (UDR)
- Media Pack
- Compatibility Matrix
- Common Microservices Load Lineup
- Security Certification Declaration
- UDR Resolved Bugs
- UDR Known Bugs

Release 2.23.1 - F78388-02, February 2023

BSF 23.1.0 Release

Updated the following sections with the details of BSF release 23.1.0:

- Binding Support Function (BSF)
- Media Pack

- Compatibility Matrix
- Common Microservices Load Lineup
- Security Certification Declaration
- BSF Known Bugs

Policy 23.1.0 Release

Updated the following sections with the details of Policy release 23.1.0:

- Policy
- Media Pack
- Compatibility Matrix
- Common Microservices Load Lineup
- Security Certification Declaration
- Policy Resolved Bugs
- Policy Known Bugs

Release 2.23.1 - F78388-01, February 2023

ATS 23.1.0 Release

Updated the following sections with the details of ATS release 23.1.0:

- Automated Testing Suite (ATS) Framework

CDCS 23.1.0 Release

Updated the following sections with the details of CDCS release 23.1.0:

- Continuous Delivery Control Server (CDCS)
- Media Pack
- Compatibility Matrix
- CDCS Resolved Bugs

CNC Console 23.1.0 Release

Updated the following sections with the details of CNC Console release 23.1.0:

- Cloud Native Configuration Console (CNC Console)
- Media Pack
- Compatibility Matrix
- Common Microservices Load Lineup
- CNC Console Resolved Bugs
- CNC Console Known Bugs

cnDBTier 23.1.0 Release

Updated the following sections with the details of cnDBTier release 23.1.0:

- Cloud Native Core cnDBTier
- Media Pack
- Compatibility Matrix

- cnDBTier Resolved Bugs

NEF 23.1.0 Release

Updated the following sections with the details of NEF release 23.1.0:

- Network Exposure Function (NEF)
- Media Pack
- Compatibility Matrix
- Common Microservices Load Lineup
- Security Certification Declaration
- NEF Resolved Bugs

NRF 23.1.0 Release

Updated the following sections with the details of NRF release 23.1.0:

- Network Repository Function (NRF)
- Media Pack
- Compatibility Matrix
- Common Microservices Load Lineup
- Security Certification Declaration
- NRF Resolved Bugs
- NRF Known Bugs

SCP 23.1.0 Release

Updated the following sections with the details of SCP release 23.1.0:

- Service Communication Proxy (SCP)
- Media Pack
- Compatibility Matrix
- Common Microservices Load Lineup
- Security Certification Declaration
- SCP Resolved Bugs
- SCP Known Bugs

SEPP 23.1.0 Release

Updated the following sections with the details of SEPP release 23.1.0:

- Security Edge Protection Proxy (SEPP)
- Media Pack
- Compatibility Matrix
- Common Microservices Load Lineup
- Security Certification Declaration
- SEPP Resolved Bugs
- SEPP Known Bugs

Common Services Resolved Bugs

Updated the following sections with the details of Common Services Resolved Bugs for release 23.1.0:

- App-Info Resolved Bugs
- ATS Resolved Bugs
- Mediation Resolved Bugs
- NRF-Client Resolved Bugs

Common Services Known Bugs

Updated the following sections with the details of Common Services Known Bugs for release 23.1.0:

- ATS Known Bugs

1 Introduction

This document provides information about new features and enhancements to the existing features for Oracle Communications Cloud Native Core network functions.

It also includes details related to media pack, common services, security certification declaration, and documentation pack. The details 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.

2
Feature Descriptions

This chapter provides a summary of new features and updates to the existing features for network functions released in Cloud Native Core release 2.23.1.

2.1 Automated Testing Suite (ATS) Framework

Release 23.1.1

No new features or feature enhancements have been introduced in this release.

Release 23.1.0

Oracle Communications Cloud Native Core, Automated Test Suite (ATS) framework 23.1.0 has been updated with the following enhancement:

- **ATS Parallel Test Execution:** Using this feature, you can perform multiple logically grouped tests simultaneously on the same System Under Test (SUT) to reduce the overall execution time of ATS. For more information, see "Parallel Test Execution" in *Oracle Communications Cloud Native Core, Automated Testing Suite Guide*.

2.2 Binding Support Function (BSF)

Release 23.1.4

No new features or feature enhancements have been introduced in this release.

Release 23.1.3

No new features or feature enhancements have been introduced in this release.

Release 23.1.2

No new features or feature enhancements have been introduced in this release.

Release 23.1.1

No new features or feature enhancements have been introduced in this release.

Release 23.1.0

Oracle Communications Cloud Native Core, Binding Support Function (BSF) 23.1.0 has been updated with the following enhancements:

- **Subscriber Activity Logging**: BSF supports Subscriber Activity Logging that allows to define a list of subscribers (identifier) that you may require to troubleshoot in the NFs and trace all logs for a specific subscriber that is separately viewed. This functionality can be used to troubleshoot problematic subscribers without enabling logs or traces that can impact all the subscribers. For more information, see Subscriber Activity Logging section in *Oracle Communications Cloud Native Core, Binding Support Function User Guide*.

- **Configurations for Pre and Post Upgrade/Install Validations**: BSF supports Upgrade Hardening, Pre and Post Flight Checks, which helps in validation checks that are required on the application, databases, and their related tables before and after the upgrade/ installation of BSF application. These pre-flight and post-flight checks ensures that all the dependent databases, tables, schema, applications are in right order for performing successful update/installation. For more information, see Configurations for Pre and Post Upgrade/Install Validations section in *Oracle Communications Cloud Native Core, Binding Support Function User Guide*.
- **Support for New ASM Parameters in Helm Chart**: BSF Aspen Mesh Custom Resource Definition (CRD) is customized by enabling or disabling various Helm parameters in the ocbsf-custom-values-servicemesh-config.yaml file. Envoy filter parameters, custom-http-stream, custom-tcpsocket-timeout, and custom-http-route are added to enable or disable HTTP Stream, TCP, and HTTP Route. For more details, see Deploying BSF with ASM section in *Oracle Communications Cloud Native core, Binding Support Function Installation, Upgrade, and Fault Recovery Guide*.
- **BSF Alarms and Observability Enhancement**:
  - **BSF Alerts**: BSF list of Alerts is updated with new ones related to BINDING_QUERY_RESPONSE, DIAM_RESPONSE_NETWORK_ERROR, DUPLICATE_BINDING_REQUEST_ERROR and NRF Client. For more information, see List of Alerts section in *Oracle Communications Cloud Native Core, Binding Support Function User Guide*.
  - **BSF Metrics**: BSF list of Metrics is updated with new ones related to NRF Client. For more information, see Metrics NRF Client section in *Oracle Communications Cloud Native Core, Binding Support Function User Guide*.

2.3 Continuous Delivery Control Server (CDCS)

Release 23.1.1

Oracle Communications CD Control Server (CDCS) 23.1.1 has been updated with the following enhancements:

- **Uplift Oracle Linux**: In this release, the base OS for CDCS VMs, and the host OS (when CDCS is installed on a bare metal server) is updated with the latest OS patches.
- **Stage View**: In this release, the Jenkins Stage View plug-in is added. This plug-in allows the user to view stage-specific logs as well as the timing information for each stage.
- **Support for New CNE Releases**: In this release, CNE 22.4.3 installation and upgrade is supported.

Release 23.1.0

Oracle Communications CD Control Server (CDCS) 23.1.0 has been updated with the following enhancements:

- **Managing CNC Console GUI**: CDCS launches the CNC Console GUI from the CDCS GUI. Use the **Manage CNCC Link** command to add a CNC Console link to the CDCS GUI. After a CNC Console link is added, the CNC Console GUI can be launched by clicking the appropriate menu on the CDCS GUI. For more information about accessing CNC Console GUI, see the "Managing CNC Console GUI Links" section in *Oracle Communications CD Control Server User Guide*.
- **Integrating LDAP Authentication**: CDCS integrates LDAP authentication for users from an external LDAP server. Once the LDAP users are integrated, you can enable or disable the LDAP user authentication from CDCS. See the Oracle Communications CD Control

Server Installation and Upgrade Guide for details on how to configure CDCS to use your LDAP server. For more information about the integration of LDAP, see the "Integrating LDAP Authentication" section in *Oracle Communications CD Control Server User Guide*.

- **Managing CDCS Rollback**: Roll back CDCS to a previous release is possible from CDCS GUI. You can use the Rollback CDCS Upgrade command to roll back to a previous release. For more information about the rollback of CDCS, see the "Rolling back a CDCS Release" section in *Oracle Communications CD Control Server User Guide*.
- **Enhancing Existing Features**:
  - **Supporting CNE Release 22.4.0 and 22.4.1**: CDCS supports installation and upgrade for CNE releases 22.4.0 and 22.4.1. CDCS GUI displays CNE 22.4.0 and 22.4.1 releases when running the **Upgrade OCCNE**, **Create New Production Site**, and **Create New Staging Site** commands. For more information about the commands, see the "Upgrading CNE at Managed Sites, Creating a New Production Site, Creating a New Staging Site" sections in Oracle Communications CD Control Server User Guide.
  - **Supporting Timeout Parameter**: CDCS supports a custom timeout value that was added to the NF Install pipeline. This value determines how long Helm will wait for the NF installation to complete. The default value is five minutes. For more information about the TIMEOUT parameter, see the "Installing NFs at Managed Sites" section in *Oracle Communications CD Control Server User Guide*.

2.4 Cloud Native Configuration Console (CNC Console)

Release 23.1.3

No new features or feature enhancements have been introduced in this release.

Release 23.1.2

No new features or feature enhancements have been introduced in this release.

Release 23.1.1

No new features or feature enhancements have been introduced in this release.

Release 23.1.0

Oracle Communications Cloud Native Configuration Console (CNC Console) 23.1.0 has been updated with the following enhancements:

- **Console Support for NWDAF**: CNC Console supports Oracle Communications Network Data Analytics Function (OCNWDAF). As part of CNC Console and NWDAF integration, features such as authentication, authorization of API/GUI requests, multicluster deployment, multi instance deployment, metrics, alerts, KPIs are now supported. For more information see the *Oracle Communications Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide* and *Oracle Communications Cloud Native Configuration Console User Guide*.
- **Documented the Name Change of CNC Console**: The acronym CNCC or CNC Console now stands for Oracle Communications Cloud Native Configuration Console.
- **Console Support for UDR ProvGW**: CNC Console supports UDR ProvGW. As part of CNC Console and UDR ProvGW, features such as authentication, authorization of API/GUI requests, multi cluster deployment, multi instance deployment, metrics, alerts, and KPIs are now supported. For more information see the *Oracle Communications Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide* and *Oracle Communications Cloud Native Configuration Console User Guide*.

- **Promxy Common Services Integration with Console**: Promxy is a Prometheus proxy that makes many shards of Prometheus appear as a single API endpoint to the user. CNC Console has enabled support for Promxy. Features such as authentication, authorization of API/GUI requests, multi cluster deployment, multi instance deployment, metrics, alerts, KPIs are now supported. For more information see the *Oracle Communications Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery* Guide. Console Log Level Screen is enhanced to display SCP logRateControl.
- Console Log Level Screen is enhanced to display SCP logRateControl.
- **Console Support for OpenSearch Dashboard and Jaeger-es**: OpenSearch lets you visualize your Elasticsearch or Opensearch data, such as application logs, Jager spans and so on, and navigate the Elastic or OpenStack to perform a variety of tasks from tracking query load to understanding the way requests flow through your apps. Jaeger-es enables you to observe old traces stored in old Elasticsearch storage that are used for troubleshooting and monitoring microservices based distributed systems. For more information, see *Oracle Communications Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide.*

2.5 Cloud Native Core cnDBTier

Release 23.1.3

No new features or feature enhancements have been introduced in this release.

Release 23.1.2

Oracle Communications Cloud Native Core, cnDBTier 23.1.2 has been updated with the following enhancements:

- **MySQL Support for Multi Threaded Applier (MTA) Feature**: The MTA feature is disabled in this release due to certain issues in the feature.

Release 23.1.1

Oracle Communications Cloud Native Core, cnDBTier 23.1.1 has been updated with the following enhancements:

- **MySQL Support for Multi Threaded Applier (MTA) Feature**: With this release, MySQL 8.0.32 supports the Multi Threaded Applier feature. NDB replication is modified to support the use of generic MySQL Server MTA mechanism. This allows independent binlog transactions to be run in parallel at a replica, thereby increasing the peak replication throughput. This is a code level enhancement and doesn't require any additional configuration.

> **Note:**
>
> cnDBTier 23.1.1 supports rollback from 23.1.1 to 23.1.0, 22.4.x, and 22.3.x.

Release 23.1.0

Oracle Communications Cloud Native Core, cnDBTier 23.1.0 has been updated with the following enhancements:

- **Support for Kubernetes Node Selector**: This feature allows the Kubernetes scheduler to determine the type of nodes in which the cnDBTier pods are to be scheduled, depending on the predefined node labels or constraints. cnDBTier uses nodeSelector and nodeAffinity

options to schedule cnDBTier pods to specific worker nodes. For more information on this feature, see *Oracle Communications Cloud Native Core, cnDBTier User Guide* and *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*.

- **Replacing SQL Commands in cnDBTier Procedures with REST APIs**: With this release, cnDBTier has replaced SQL commands in cnDBTier procedures with REST APIs. This will restrict the access to the MySQL credentials and avoid the manual errors of breaking the replication between other remote sites.
- **Script to Change cnDBTier Passwords**: With this release, cnDBTier provides a bash script to change cnDBTier passwords. This script can be used to change one or more cnDBTier passwords of stand alone and georeplicated clusters. For more information about this feature, see the "Changing cnDBTier Passwords" section in *Oracle Communications Cloud Native Core, cnDBTier User Guide*.
- **Support for New Version of MySQL Cluster Software**: The Oracle MySQL Cluster Database software is upgraded to 8.0.32 in this release.

> **Note:**
>
> cnDBTier 23.1.x supports rollback from 23.1.x to 22.3.x and 22.4.x (with service account only). It doesn't support rollback to 22.4.x without service account.

2.6 Cloud Native Environment (CNE)

> **Note:**
>
> The procedure to update OpenStack credentials is revised in the 23.1.4 User Guide. If you are updating OpenStack credentials on other versions of 23.1.x, refer to the latest procedure from 23.1.4 *Oracle Communications Cloud Native Core, Cloud Native Environment User Guide*.

Release 23.1.4

There are no new features or feature enhancements in this release.

Release 23.1.3

Oracle Communications Cloud Native Core, Cloud Native Environment (CNE) 23.1.3 has been updated with the following enhancements:

New Versions of Common Services: The following OpenSearch services are upgraded in this release:

- Oracle OpenSearch - 2.3.0
- Oracle OpenSearch Dashboard - 2.3.0
- Fluentd OpenSearch - 1.16

These upgrades provide number of new features offered by OpenSearch. For example, Fluent Bit is replaced with Fluentd OpenSearch. That is, log forwarding mechanism is changed from fluent-bit to fluentd-openSearch. The other changes in the OpenSearch stack are as follows:

- There are five OpenSearch data nodes created by default.

- Upgrade from 22.4.x to 23.1.3 has Elastic Search to store old index data and OpenSearch to ingest new data.
- CNE Environment upgrading from 23.1.1 and 23.1.2 requires OpenSearch Dashboard filters to be updated in saved queries.

OpenSearch and Fluentd Performance Considerations: OpenSearch and Fluentd are used for log ingestion. The performance of these services depends on the rate at which log forwarding happens, rate of ingestion, and log retention periods. It is advised to collect the aforementioned metrics from different components that are running in CNE cluster and ingesting logs to OpenSearch. The resource requirements of OpenSearch differs according to the collection of these metrics.

To get the complete list of third party services and their versions, refer to the `dependencies_23.1.3.tgz` file provided as part of the software delivery package.

Release 23.1.2

There are no new features or feature enhancements in this release.

Release 23.1.1

Oracle Communications Cloud Native Core, Cloud Native Environment (CNE) 23.1.1 has been updated with the following enhancements:

- **Egress NAT with Multiple Egress Network Support**: In this release, Egress NAT feature is extended to support Egress network routing. With this enhancement, any pod that performs egress requests can send egress message to multiple networks by providing egress annotations for pods. For more details on configuring this feature, see *Oracle Communications Cloud Native Core, Cloud Native Environment User Guide*.
- **Upgrade Consideration**: The `kube_network_node_prefix_value` variable must be defined at the time of installation only. Modifying this variable value during an upgrade leads to upgrade failures. Therefore, retain the same variable value that is assigned at the time of installation. For information on verifying the `kube_network_node_prefix_value` value, see the "Preupgrade Config Files Check" section of *Oracle Communications Cloud Native Core, Cloud Native Environment Upgrade Guide*.

Release 23.1.0

Oracle Communications Cloud Native Core, Cloud Native Environment (CNE) 23.1.0 has been updated with the following enhancements:

- **Productize Oracle OpenSearch as Elasticsearch Replacement:** This release replaces Elasticsearch with Oracle OpenSearch as a log ingestion tool. Therefore, Elasticsearch and Kibana are no more supported and are replaced with Oracle OpenSearch and Oracle OpenSearch Dashboard, respectively. Oracle internally manages its own copy of OpenSearch called Oracle OpenSearch and OpenSearch Dashboard called Oracle OpenSearch Dashboard. For more information, see *Oracle Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide*.
  - **Upgrade Impact**: While performing an upgrade from 22.4.x to 23.1.0, the upgrade procedure offers an option to perform the upgrade with or without Elasticsearch. Elasticsearch and its related components are not removed when you perform an upgrade from 22.4.x to 23.1.0 to ensure any logging and metric data that is available in the preupgrade version of CNE 22.4.x is not lost. Both Elasticsearch and OpenSearch are available in CNE 23.1.0, however all new logs, after your upgrade to 23.1.0, is ingested in OpenSearch. You can access all the old logs using Elasticsearch and Kibana interface until the data expire. For more information, see *Oracle*

Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide.

- **Replace Deprecated Kubernetes Pod Security Policy**: PodSecurityPolicy (PSP) is a built-in admission controller that allows a cluster administrator to control security-sensitive aspects of pod specification. As Kubernetes has deprecated its PSP, CNE has adopted to a new framework called Kyverno. Kyverno provides security policies for CNE clusters and all PSP based access or security policies are upgraded with Kyverno. For more information on this framework, see *Oracle Communications Cloud Native Core, Cloud Native Environment User Guide* and *Oracle Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide*.
- **Automated Backup and Restore for CNE**: In this release, CNE provides option to backup and restore CNE, including Bastion Hosts, using Velero. Velero provides tools to take on-demand backup and restore the Kubernetes cluster resources and persistent volumes. Velero runs as part of CNE cluster and can be administered from CLI interface. This feature helps to better manage CNE upgrades and replicate clusters for testing purposes. For more information about CNE backup and restore, see *Oracle Communications Cloud Native Core, Cloud Native Environment User Guide*.
  - **Upgrade Impact**: Velero is not installed as a part of the installation and upgrade process and needs to be activated post CNE installation or upgrade. This is due to Velero's dependency on block storage to store backups and the block storage must be s3 compatible. For more information on Velero activation process, see *Oracle Communications Cloud Native Core, Cloud Native Environment User Guide* and *Oracle Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide*.
- **New Versions of Common Services**: The following common services are upgraded in this release:
  - Helm - 3.9.4
  - Kubernetes - 1.24.6
  - containerd - 1.6.4
  - Calico - 3.23.3
  - MetalLB - 0.13.7
  - Prometheus - 2.39.1
  - Grafana - 9.1.7
  - Jaeger - 1.39.0
  - Istio - 1.15.3
  - Kyverno - 1.7.3
  - cert-manager - 1.10.0

You can find the complete list of third party services and their versions in the *dependencies_23.1.0.tgz* file provided as part of the software delivery package.

2.7 Network Exposure Function (NEF)

Release 23.1.4

No new features or feature enhancements have been introduced in this release.

Release 23.1.3

No new features or feature enhancements have been introduced in this release.

Release 23.1.2

No new features or feature enhancements have been introduced in this release.

Release 23.1.1

No new features or feature enhancements have been introduced in this release.

Release 23.1.0

Oracle Communications Cloud Native Core, Network Exposure Function (NEF) 23.1.0 has been updated with the following enhancements:

- **Support for Traffic Influence**: Traffic Influence is mainly used by AFs to influence the routing decisions on the user plane traffic. It allows the AF to decide the routing profile and the route for data plane from UE to network in a particular PDU session. For more information, see *Oracle Communications Cloud Native Core, Network Exposure Function Installation, Upgrade, and Fault Recovery Guide* and *Oracle Communications Cloud Native Core, Network Exposure Function User Guide.*
- **Supports Converged SCEF-NEF**: With the introduction of this feature, when a UE request is sent from a 4G network, MME node detects this event and sends the notification to NEF. As NEF is not capable of accepting the diameter requests, a Diameter Gateway is used to allow the diameter traffic to NEF. For more information, see *Oracle Communications Cloud Native Core, Network Exposure Function Installation, Upgrade, and Fault Recovery Guide, Oracle Communications Cloud Native Core, Network Exposure Function User Guide,* and *Oracle Communications Cloud Native Core, Network Exposure Function Troubleshooting Guide.*

2.8 Network Repository Function (NRF)

Release 23.1.4

No new features or feature enhancements have been introduced in this release.

Release 23.1.3

No new features or feature enhancements have been introduced in this release.

Release 23.1.2

No new features or feature enhancements have been introduced in this release.

Release 23.1.1

Oracle Communications Cloud Native Core, Network Repository Functions (NRF) 23.1.1 has been updated with the following enhancement:

- **Support for Configurable Port and Routing Parameter Selection**: NRF provides a configurable option to select a port, if not configured explicitly, either from IPEndpoint or using the scheme attribute of NfService. Additionally, NRF allows to configure the preferred routing attribute in case more than one of the following attributes is present in the NfProfile or NfService:

  - IPv4 (ipv4Addresses from IpEndpoint of NfService if present, or ipv4Addresses of NfProfile)
  - IPv6 (ipv6Addresses from IpEndpoint of NfService if present, or ipv6Addresses of NfProfile)
  - FQDN (fqdn of NfService if present, or fqdn of NfProfile)

For more information about the feature, see "Configurable Port and Routing Parameter Selection" in *Oracle Communications Cloud Native Core, Network Repository Function User Guide*.

Release 23.1.0

Oracle Communications Cloud Native Core, Network Repository Functions (NRF) 23.1.0 has been updated with the following enhancements:

- **Support for TLS 1.2 SNI Extension**: NRF supports Server Name Identification (SNI) header for TLS handshake messages to identify the server to which the connection must be established. For more information about the feature, see "TLS SNI Header Validation" in *Oracle Communications Cloud Native Core, Network Repository Function User Guide*.
- **Pod Protection Support for NRF Subscription Microservice**: NRF Subscription microservice is responsible for the NfStatusSubscribe, NfStatusUnsubscribe, and NfStatusNotify service operations. These service operations send notifications and requests to Subscription microservice and thus lead the Subscription microservice to congested or overload condition. This feature protects the Subscription microservice from overload situations and maintain the overall health. For more information about the feature, see "Subscription Microservice Pod Protection" in *Oracle Communications Cloud Native Core, Network Repository Function User Guide*.
- **Support for notification-type Nfdiscover Attribute**: NRF supports notification-type as a query parameter in GET Discovery API to provide default notification subscriptions that were registered in the NFProfile or NFService of the NF Instances being discovered in the response. Along with notification-type, n1-msg-class and n2-info-class discovery query attributes are also supported.
- **Support for Auditing the Availability of NRF Tables**: NRF detects any inconsistency in the system at early stage of installation and reports the same. The validations are done during the preinstallation and postinstallation. For more information about the feature, see "Audit NRF Database Tables" in *Oracle Communications Cloud Native Core, Network Repository Function User Guide*.
- **Support for NodeSelector for NRF Microservices**: NRF allows the Kubernetes scheduler to determine the type of nodes in which the NRF pods are scheduled, depending on the predefined node labels or constraints. Node selector is a basic form of cluster node selection constraint. It allows you to define the node labels (constraints) in the form of key-value pairs. When the nodeSelector feature is used, Kubernetes assigns the pods to only the nodes that match with the node labels you specify. For more information about the feature, see "Node Selector" in *Oracle Communications Cloud Native Core, Network Repository Function User Guide*.
- **Support for using Last Known NFProfile during Replication Down**: NRF considers the last known NfProfiles of remote NRFs for any service operations during platform maintenance, network issues, or for any other reason, if the replication channels go down. For more information about the feature, see "Using Last Known NfProfile during Replication Down" in *Oracle Communications Cloud Native Core, Network Repository Function User Guide*.
- **Support for Using App-Info Microservice to Fetch DB Replication Status**: NRF queries appInfo microservice for fetching database replication channel status instead of

Database Monitor service. For more information about the feature, see "Fetching the Database Replication Channel Status Using appinfo Microservice" in *Oracle Communications Cloud Native Core, Network Repository Function User Guide*.

- **Support for Ignoring Unknown Attribute in NFDiscovery Search Query**: NRF supports configuring of NFDiscover search query attributes that can be ignored. Instead of sending 400 bad request for such attributes, NRF ignores the configured attributes and process the request. For more information about the feature, see "Ignore Unknown Attribute in NFDiscover Search Query" in *Oracle Communications Cloud Native Core, Network Repository Function User Guide*.

2.9 Network Slice Selection Function (NSSF)

Release 23.1.2

No new features or feature enhancements have been introduced in this release.

Release 23.1.1

Oracle Communications Cloud Native Core, Network Slice Selection Function (NSSF) 23.1.1 has been updated with the following enhancement:

- **Functionality to Delete Subscription When Notification Request Gets a 404 Subscription Not Found Response**: This feature, an enhancement to NSSF Notify Service Operation, updates the NF Service Consumer (for example, AMF) of any change in status. When it is enabled, it eliminates the unnecessary delay in response by logging the error and deleting the subscription whenever AMF sends the '404 Subscription Not Found' response. For more information, see "Functionality to Delete Subscription When Notification Request Gets a 404 Subscription Not Found Response" in *Oracle Communications Cloud Native Core, Network Slice Selection Function User Guide*.

Release 23.1.0

Oracle Communications Cloud Native Core, Network Slice Selection Function (NSSF) 23.1.0 has been updated with the following enhancements:

- **Support for DNS SRV Based Selection of SCP in NSSF:** This enhancement enables NSSF to learn SCP configuration based on DNS SRV based FQDN, in addition to the already existing static manual configuration by the operator. Additionally, it extends support for AlternateRoute Service, which allows the configuration of as many dynamic sets of SPC instances in NSSF in contrast to only one static configuration in the previous scenarios. For more information, see "DNS SRV Based Selection of SCP in NSSF" in *Oracle Communications Cloud Native Core, Network Slice Selection Function User Guide*.
- **NSSF ATS Golden Configuration**: This enhancement gives the ability to run test cases defined by NSSF on customer's Golden Configuration. For more information, see *Oracle Communications Cloud Native Core, Automated Testing Suite Guide*.
- **Configuration of Network Policies**: Network policies allow ingress or egress rules to be defined based on Kubernetes resources such as Pod, Namespace, IP, and Ports. These rules are selected based on Kubernetes labels in the application. These network policies enforce access restrictions for all the applicable data flows except communication from Kubernetes node to pod for invoking container probe. For more information, see "Configuring Network Policies" in *Oracle Communications Cloud Native Core, Network Slice Selection Function Installation, Upgrade, and Fault Recovery Guide*.

2.10 Policy

Release 23.1.8

No new features or feature enhancements have been introduced in this release.

Release 23.1.7

Oracle Communications Cloud Native Core, Converged Policy 23.1.7 has been updated with the following enhancement:

- **Enhancements to Audit Configurations**: Audit Service configurations in CNC Policy is enhanced with addition of a new parameter *Minimum Audit Attempts* to PCF Session Management, Binding Service, and Audit Service pages on CNC Console. These enhanced configurations resolve the issues related to identification and deletion of stale records by Audit Service. For more information, see "Configuring CNC Policy Using CNC Console" in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.

Release 23.1.6

No new features or feature enhancements have been introduced in this release.

Release 23.1.5

No new features or feature enhancements have been introduced in this release.

Release 23.1.4

No new features or feature enhancements have been introduced in this release.

Release 23.1.3

No new features or feature enhancements have been introduced in this release.

Release 23.1.2

No new features or feature enhancements have been introduced in this release.

Release 23.1.1

No new features or feature enhancements have been introduced in this release.

Release 23.1.0

Oracle Communications Cloud Native Core, Converged Policy 23.1.0 has been updated with the following enhancements:

- **Pending Transaction on N15 for AM and UE Policy Association**: Policy supports pending transactions at the N15 interface to handle race conditions in a deterministic manner. For more information on how to configure this feature using CNC Console, see the "Pending Transaction on N7 and N15 Interface" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.
- **Timer Handling Enhancements for AM and UE Policy Service**: Policy is enhanced to support timer handling for AM and UE policy. For more information on how to configure this feature using CNC Console, see the "SBI Timer Handling" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.

- **Detection and Handling of Late Arrival Requests on the N15 Interface for AM and UE Policy**: Policy is enhanced to support the detection and handling of late arrival requests on the N15 interface for AM and UE Policy to detect the response time for the components received in the headers from the Ingress Gateway. For more information on how to configure this feature using CNC Console, see the "Detection and Handling of Late Arrival Requests" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.
- **Consistent UDR Updates Using ETag**: When two different Policies are connected to UDR in a georedundant setup and both are updating the UsageMonData for the same subscriber simultaneously, there is the possibility of data loss as the update can overwrite each other. ETag (Entity Tag) support helps to make sure that the update is successful only when the consumer has the latest set of data. For more information on how to configure this feature using CNC Console, see the "Consistent UDR Updates using ETag" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.
- **SCP Selection When Priority is Same**: Policy is enhanced to support a weight factor when the priorities of the peers are the same. This weight factor will be the deciding factor as to which peer is to be picked when the priorities of the peers are the same. For more information on how to configure this feature, see the "SCP Configuration" section in *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide*.
- **Session Retry SM Service Notification Enhancement**: Policy supports Session Retry for SMF notification to use servicename for SMF discovery and selection. For more information, see the "Support for Session Retry and Alternate Route Service" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.
- **Session Retry Configuration to Retry SUBSCRIPTION towards UDR as an INITIAL or SUBSEQUENT Message**: Policy supports Session Retry in Policy to provide configuration to Retry SUBSCRIPTION towards UDR as an INITIAL or SUBSEQUENT message. For more information, see the "Support for Session Retry and Alternate Route Service" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.
- **Notification Request Retries for AM and UE Policy**: Policy is enhanced to support retry with NF Sets, binding headers, Server-PCF as an HTTP Client, and Notification Producer for AMF as a notification consumer for AM and UE policy. For more information, see the "Support for Session Retry and Alternate Route Service" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.
- **Concurrency Handling for SM Update SM Clean**: Policy uses the Bulwark service to handle the concurrent requests coming from other Policy services. The Bulwark service integrates with SM service to handle the concurrent requests for the SM Update and the SM Clean procedures. The SM service integration with Bulwark service handles the concurrent requests for the same subscriber in a concurrent and efficient manner. For more details, see "Support for Concurrency Handling using Bulwark Service" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.
- **Support for State Variables in Policy**: Policy provides state variables support for SM Service, AM Service, and UE Policy Service. The State variables hold the intermediate state of the policy evaluation. The state variables are defined by the policy writer that can be set within a policy action to be used at a later time during policy rule execution (in either conditions or actions). The names of these variables are not predefined and are determined by the policy writer. For more details, see "State Variables in Policy" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.
- **Support for Successful Resource Allocation for PCC Rules**: The Successful Resource Allocation (SRA) enables Policy to get the status of the Policy and Charging Control Rule (PCC Rules) that are successfully installed and validated by Session Management Function (SMF). Policy writer can take appropriate action based on the successful

activation of a rule. For example, a Policy writer can hold updating the installed PCC rule unless SRA is applied at SMF. For more details, see "Support for Successful Resource Allocation for PCC Rules" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.

- **Support for MCPTT Features**: This feature enables Policy and Charging Rules Function (PCRF) support for MCPTT related QoS Class Identifier (QCI)s, and MCPTT specific features such as Priority sharing and Preemption. PCRF enables MCPTT for a session based on the supported features exchanged between the Policy and Charging Enforcement Function (PCEF)/Application Function (AF) and PCRF (dynamic discovery of supported features). For more details, see "Support for MCPTT Features" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.
- **Support for Overload Control SBI - Threshold Configuration Using CNC Console**: Policy supports configuration of Overload Control Thresholds based on active threshold profiles using CNC Console. For more details, see "Overload Control Threshold Configuration" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.
- **AMF Selection for Namf-comm Subscription**: Policy supports discovering AMF as a producer based on AMF SetID and AMF Region ID, which are extracted from Globally Unique AMF Identifier (GUAMI). This aids in transfering the UE Policy to UE through AMF and sending initial subscription request to AMF during UE Policy Transfer request. For more details, see "UE Policy Enhancements" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.
- **Configurations for Pre and Post Upgrade/Install Validations**: Policy supports Upgrade Hardening, Pre and Post Flight Checks, which helps in validation checks that are required on the application, databases, and its related tables before and after the upgrade/ installation of BSF application. These pre-flight and post-flight checks ensures that all the dependent databases, tables, schema, applications are in right order for performing successful update/installation. For more information, see "Configurations for Pre and Post Upgrade/Install Validations" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.
- **Support for New ASM Parameters in Helm Chart**: Policy Aspen Mesh Custom Resource Definition (CRD) is customized by enabling or disabling various Helm parameters in the *occnp-custom-values-servicemesh-config.yaml* file. Envoy filter parameters custom-http-stream, custom-tcpsocket-timeout and custom-http-route are added to enable or disable HTTP Stream, TCP and HTTP Route. For more details, see "Deploying Policy with ASM" section in *Oracle Communications Cloud Native core, Converged Policy Installation, Upgrade, and Fault Recovery Guide*.
- **Audit Service Multi-pod Support**: Audit Service is responsible for auditing the database to monitor stale records, and either notify or clean up these stale records. Audit service with single pod deployment makes it neither scalable nor highly available. Now, Policy supports Audit service multiple pods by using Audit Schedule. Audit Schedule helps to effectively manage and plan the audit service on the registered services. For more information, see "Audit Service" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.

2.11 Service Communication Proxy (SCP)

Release 23.1.3

No new features or feature enhancements have been introduced in this release.

Release 23.1.2

No new features or feature enhancements have been introduced in this release.

Release 23.1.1

No new features or feature enhancements have been introduced in this release.

Release 23.1.0

Oracle Communications Cloud Native Core, Service Communication Proxy (SCP) 23.1.0 has been updated with the following enhancements:

- **Routing Support for NEF Services**: This feature enables SCP to determine Network Exposure Function (NEF) profile registration and updates from Network Repository Function (NRF) and create routing and alternate-routing rules for NEF services. For more information, see "Routing Support for NEF Services" in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.
- **Extension of HTTP Status Code List for Rerouting**: SCP can reroute a message request based on the user-provided configurable error codes. For more information, see "Extension of HTTP Status Code List for Rerouting" in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.
- **ATS Parallel Test Execution**: This is an ATS Framework feature. Using this feature, you can perform multiple logically grouped tests simultaneously on the same System Under Test (SUT) to reduce the overall execution time of ATS. For more information, see "Parallel Test Execution" in *Oracle Communications Cloud Native Core, Automated Testing Suite Guide*.
- **Support for NF Status Notifications with Partial NF Profile**: SCP supports partial profile processing, that is, Notification with profileChanges processing. For more information, see "SCP Interactions with NRF" in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.
- **Host Preference for Egress Message Requests**: This feature enables SCP to determine the host type to be included in the egress message requests based on the 3gpp-Sbi-Target-apiRoot header, hostPreference REST API configuration, and learned Network Function (NF) profile from Network Repository Function (NRF). For more information, see "Host Preference for Egress Message Requests" in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.
- **Enhanced 5G SBI Message Failure Handling**: This enhancement enables SCP to add a server header with its Fully Qualified Domain Name (FQDN) for the self-generated error responses when SCP does not receive a server header in an error response from a producer NF. If SCP is deployed with Aspen Service Mesh (ASM), SCP adds a server header with its FQDN in the error responses received from the service mesh sidecar. For more information, see "Enhanced 5G SBI Message Failure Handling" in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.

2.12 Security Edge Protection Proxy (SEPP)

Release 23.1.4

No new features or feature enhancements have been introduced in this release.

Release 23.1.3

No new features or feature enhancements have been introduced in this release.

Release 23.1.2

No new features or feature enhancements have been introduced in this release.

Release 23.1.1

No new features or feature enhancements have been introduced in this release.

Release 23.1.0

Oracle Communications Cloud Native Core, Security Edge Protection Proxy (SEPP) 23.1.0 has been updated with the following enhancements:

- **Rate Limiting for Ingress Roaming Signaling per Remote SEPP Set**: This feature provides ingress request rate limiting on N32 Interface based on Remote SEPP Set to throttle messages from the Remote SEPP sending more than configured limit for the Remote SEPP Set. There can be scenarios where the flood of messages at Remote SEPP Set level need to be controlled.
  With this feature, SEPP secures the network when aggregated traffic at the Remote SEPP level exceeds the allowed traffic rate limit. If the traffic exceeds the allowed traffic rate limit, SEPP does not process the traffic and responds with an error code. The rate limiting functionality at SEPP allows an operator to configure the acceptable traffic rate from a consumer NF instance.

  SEPP enables users to configure the maximum number of incoming messages at a given duration. For more information about the feature, see the "Rate Limiting for Ingress Roaming Signaling per Remote SEPP Set" section in Oracle Communications Cloud Native Core, Security Edge Protection Proxy User Guide, Oracle Communications Cloud Native Core, Security Edge Protection Proxy REST API Specification Guide, and "Configuration Parameters" section in *Oracle Communications Cloud Native Core, Security Edge Protection Proxy Installation and Upgrade Guide*.
- **Support for 3-Site Georedundancy**: The SEPP architecture supports georedundant deployments to ensure high availability and redundancy. It offers 3-site georedundancy to ensure service availability when one of the SEPP sites is down. When SEPP is deployed in a three-site georedundant setup, all the three SEPP sites work in an Active state. For more information about the feature, see the "Support for 3-Site Georedundancy" section in *Oracle Communications Cloud Native Core, Security Edge Protection Proxy User Guide*.
- **Steering of Roaming (SOR)**: SOR is deployed as a roaming management solution intended for optimizing roaming cooperation between operators. It allows flexible network selection management for outbound roamers to stimulate an appropriate roaming network choice for subscribers. SEPP supports the SOR feature to provide better roaming experience to the customers.
  Based on the redirection of response from SOR platform, the feature can be implemented in the following two modes.
  - Redirection Disabled Mode (Passive Mode): In this mode, SEPP supports sending UDM traffic to an asserted UDM when traffic steering (Steering of Roaming) platform fails to route the message. SOR either connects to the required subscriber or returns the location of the required subscriber to the home SEPP.
  - Redirection Enabled Mode (Active Mode): In this mode, SEPP supports directing UDM messages to a Steering of Roaming Application Server.

  For more information about the feature, see the "Steering of Roaming (SOR)" section *in Oracle Communications Cloud Native Core, Security Edge Protection Proxy User Guide* and *Oracle Communications Cloud Native Core, Security Edge Protection Proxy REST API Specification Guide*.

- **Cat 2 - Validation of CSEPP PLMN ID**: Cat 2 – Network ID Validation feature allows the user to validate the PLMN ID of Producer SEPP and Consumer SEPP in the SBI Request Messages over N32 Interface in SEPP Mode as well as in Roaming Hub Mode. Existing CAT 2 Network ID Validation feature is enhanced to support Validation of CSEPP PLMN ID on consumer and Producer SEPP against the configured list of PLMN IDs (Local as well as Remote SEPP) for any Ingress or Egress messages which can contain this information.

  Example: Any message configured to validate CSEPP PLMN ID, that contains the servingNetworkName Body IE parameter must be used for this validation. For more information about the feature, see the "CAT 2 - Network ID Validation Feature" section in *Oracle Communications Cloud Native Core, Security Edge Protection Proxy User Guide* and *Oracle Communications Cloud Native Core, Security Edge Protection Proxy REST API Specification Guide*.
- **SEPP Automated Testing Suite (ATS) is Configured to Support Aspen Service Mesh**: SEPP Automated Testing Suite (ATS) is configured to Support Aspen Service Mesh (ASM). The new ASM related test cases are added in ATS and existing ATS cases are updated to support both ASM and non-ASM platform. For more information about the feature, see the *Oracle Communications Cloud Native Core, Automated Testing Suite Guide*.
- **Support 62K MPS per SEPP Instance**: SEPP is enhanced and optimized the micro services code to support 62K MPS per SEPP instance. For more information on benchmarking details, see *Oracle Communications Cloud Native Core, Security Edge Protection Proxy Benchmarking Guide*.
- **SEPP Performance with Bare Minimum Resources**: As part of SEPP resource footprint optimization, SEPP's minimum performance is tested on bare-minimum resource footprint per microservice. For more information about the feature, see the "Resource Requirements" section in *Oracle Communications Cloud Native Core, Security Edge Protection Proxy Installation, and Upgrade Guide*.

2.13 Unified Data Repository (UDR)

Release 23.1.3

No new features or feature enhancements have been introduced in this release.

Release 23.1.2

No new features or feature enhancements have been introduced in this release.

Release 23.1.1

No new features or feature enhancements have been introduced in this release.

Release 23.1.0

Oracle Communications Cloud Native Core, Unified Data Repository (UDR) 23.1.0 has been updated with the following enhancements:

- **ETag (Entity Tag) Support for UDR**: When two different Cloud Native Policy and Charging Rules Function (cnPCRF) are connected to UDR in a georedundant setup and both the PCRF are updating the UsageMonData for the same subscriber simultaneously, there is possibility of data loss as the updates can overwrite each other. ETag support for UDR helps to make sure that the update is successful only when the consumer has the latest set of data, which is determined by the ETag value received at UDR. When you send a GET sm-data request to get the UsageMonData, the ETag header with default value 0 is

attached with the sm-data and added in the GET sm-data response. This ETag value is used in PUT or PATCH update request with if-match header to maintain concurrency control. For more information about the feature, see "ETag support for UDR" section in *Oracle Communications Cloud Native Core, Unified Data Repository User Guide*.

- **ETag Notifications**: UDR sends updated ETag notifications header to the consumer about the current state of the usage monitoring data. This enables the consumer to update the ETag values in the subsequent update operations. For more information about the feature, see "ETag support for UDR" section in *Oracle Communications Cloud Native Core, Unified Data Repository User Guide*.
- **Controlled Shutdown of an Instance**: UDR supports controlled shutdown to provide the partial or complete isolation of the site from the network so that the operator can perform necessary recovery procedures. For more information about the feature, see "Controlled Shutdown of an Instance" section in *Oracle Communications Cloud Native Core, Unified Data Repository User Guide*.
- **Auto Enrollment**: Consumer NFs such as cnPCRF need UDR to enroll the subscriber record with policy data sent on the N36 interface. This is required for subscribers in roaming scenarios, where cnPCRF does a PATCH operation to update the subscriber data. Auto enrollment enables UDR to auto enroll the subscriber if the subscriber record does not exist. Auto enrollment also supports UDR in creating mandatory attribute smPolicySnssaiData with configured default values when NF such as cnPCRF does not include smPolicySnssaiData attribute in sm-data.
  The auto enrollment feature in UDR supports the auto provisioning of subscribers for the following signaling APIs:
  - PATCH on SessionManagementPolicyData
  - PUT on UsageMonitoringInformation

  For more information about the feature, see "Auto Enrollment" section in *Oracle Communications Cloud Native Core, Unified Data Repository User Guide*.
- **CNC Console Support for Provision Gateway Configurations**: CNC Console support is provided for Provision Gateway to configure the parameters. For more information about the feature, see "Configuring Provisioning Gateway using CNC Console" section in *Oracle Communications Cloud Native Core, Unified Data Repository User Guide*.
- **Support for Application Log Collection for UDR ATS**: Application log collection enables ATS to collect logs from System Under Test (SUT) when there are scenario failures. The user can set log level to one of values mentioned below:
  - WARN
  - INFO
  - DEBUG
  - ERROR
  - TRACE

  For more information about the feature, see "UDR Application Log Collection" section in *Oracle Communications Cloud Native Core, Automated Testing Suite Guide*.
- **Aspen Service Mesh (ASM)** enhancement support for UDR: The following enhancements are supported:
  - Transmission Control Protocol (TCP) Connection in destination rules
  - TCP connection and The Hypertext Transfer Protocol (HTTP) stream in envoy filters
  - HTTP route in virtual service

For more information about the feature, see "ASM Specific Configuration" section in *Oracle Communications Cloud Native Core, Unified Data Repository User Guide*.

3
Media and Documentation

3.1 Media Pack

This section lists the media package for Oracle Communications Cloud Native Core 2.23.1. To download the media package, see MOS.

To learn how to access and download the media package from MOS, see Accessing NF Documents on 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 Oracle Communications Cloud Native Core 2.23.1

Description	NF Version	ATS Version	Upgrade Supported
Oracle Communications Cloud Native Core, Binding Support Function (BSF)	23.1.4	23.1.4	BSF 23.1.4 supports fresh installation and upgrade from 22.3.x, 22.4.x, and 23.1.x to 23.1.4. For more information, see *Oracle Communications Cloud Native Core, Binding Support Function Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Binding Support Function (BSF)	23.1.3	23.1.3	BSF 23.1.3 supports fresh installation and upgrade from 22.3.x, 22.4.x, and 23.1.x to 23.1.3. For more information, see *Oracle Communications Cloud Native Core, Binding Support Function Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Binding Support Function (BSF)	23.1.2	23.1.2	BSF 23.1.2 supports fresh installation and upgrade from 22.3.x, 22.4.x, and 23.1.x to 23.1.2. For more information, see *Oracle Communications Cloud Native Core, Binding Support Function Installation, Upgrade, and Fault Recovery Guide*.

Table 3-1 (Cont.) Media Pack Contents for Oracle Communications Cloud Native Core 2.23.1

Description	NF Version	ATS Version	Upgrade Supported
Oracle Communications Cloud Native Core, Binding Support Function (BSF)	23.1.1	23.1.1	BSF 23.1.1 supports fresh installation and upgrade from 22.3.x, 22.4.x, and 23.1.0 to 23.1.1. For more information, see *Oracle Communications Cloud Native Core, Binding Support Function Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Binding Support Function (BSF)	23.1.0	23.1.0	BSF 23.1.0 supports fresh installation and upgrade from 22.3.x and 22.4.x to 23.1.0. For more information, see *Oracle Communications Cloud Native Core, Binding Support Function Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications CD Control Server (CDCS)	23.1.1	NA	CD Control Server 23.1.1 supports fresh installation and upgrade from 22.4.x and 23.1.0 to 23.1.1. For more information, see *Oracle Communications CD Control Server Installation and Upgrade Guide*.
Oracle Communications CD Control Server (CDCS)	23.1.0	NA	CD Control Server 23.1.0 supports fresh installation and upgrade from 22.4.x to 23.1.0. For more information, see *Oracle Communications CD Control Server Installation and Upgrade Guide*.
Oracle Communications Cloud Native Configuration Console (CNC Console)	23.1.3	NA	CNC Console 23.1.3 supports fresh installation and upgrade from 22.3.x, 22.4.x, and 23.1.x to 23.1.3. For more information, see *Oracle Communications Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Configuration Console (CNC Console)	23.1.2	NA	CNC Console 23.1.2 supports fresh installation and upgrade from 22.3.x, 22.4.x, and 23.1.x to 23.1.2. For more information, see *Oracle Communications Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Configuration Console (CNC Console)	23.1.1	NA	CNC Console 23.1.1 supports fresh installation and upgrade from 22.3.x, 22.4.x, and 23.1.x to 23.1.1. For more information, see *Oracle Communications Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide*.

Table 3-1 (Cont.) Media Pack Contents for Oracle Communications Cloud Native Core 2.23.1

Description	NF Version	ATS Version	Upgrade Supported
Oracle Communications Cloud Native Configuration Console (CNC Console)	23.1.0	NA	CNC Console 23.1.0 supports fresh installation and upgrade from 22.3.x and 22.4.x to 23.1.0. For more information, see *Oracle Communications Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide.*
Oracle Communications Cloud Native Core, Cloud Native Environment (CNE)	23.1.4	NA	CNE 23.1.4 supports fresh installation and upgrade from 22.4.x and 23.1.x to 23.1.4. For more information, see *Oracle Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Cloud Native Environment (CNE)	23.1.3	NA	CNE 23.1.3 supports fresh installation and upgrade from 22.4.x and 23.1.x to 23.1.3. For more information, see *Oracle Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Cloud Native Environment (CNE)	23.1.2	NA	CNE 23.1.2 supports fresh installation and upgrade from 22.4.x and 23.1.x to 23.1.2. For more information, see *Oracle Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Cloud Native Environment (CNE)	23.1.1	NA	CNE 23.1.1 supports fresh installation and upgrade from 22.4.x and 23.1.0 to 23.1.1. For more information, see *Oracle Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Cloud Native Environment (CNE)	23.1.0	NA	CNE 23.1.0 supports fresh installation and upgrade from 22.4.x to 23.1.0. For more information, see *Oracle Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide.*
Oracle Communications Cloud Native Core, cnDBTier	23.1.3	NA	cnDBTier 23.1.3 supports fresh installation and upgrade from 22.3.x, 22.4.x, and 23.1.x to 23.1.3. For more information, see *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*.

Table 3-1 (Cont.) Media Pack Contents for Oracle Communications Cloud Native Core 2.23.1

Description	NF Version	ATS Version	Upgrade Supported
Oracle Communications Cloud Native Core, cnDBTier	23.1.2	NA	cnDBTier 23.1.2 supports fresh installation and upgrade from 22.3.x, 22.4.x, and 23.1.x to 23.1.2. For more information, see *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, cnDBTier	23.1.1	NA	cnDBTier 23.1.1 supports fresh installation and upgrade from 22.3.x, 22.4.x, and 23.1.0 to 23.1.1. For more information, see *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, cnDBTier	23.1.0	NA	cnDBTier 23.1.0 supports fresh installation and upgrade from 22.3.x and 22.4.x to 23.1.0. For more information, see *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Converged Policy (Policy)	23.1.8	23.1.4	Policy 23.1.8 supports fresh installation and upgrade from 22.3.x, 22.4.x, and 23.1.x to 23.1.8. For more information, see *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide*.

Table 3-1 (Cont.) Media Pack Contents for Oracle Communications Cloud Native Core 2.23.1

Description	NF Version	ATS Version	Upgrade Supported
Oracle Communications Cloud Native Core, Converged Policy (Policy)	23.1.7	23.1.2	Policy 23.1.7 supports fresh installation and upgrade from 22.3.x, 22.4.x, and 23.1.x to 23.1.7. For more information, see *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide*. **Note :** This release is an SM only release, not applicable to UE and AM.
Oracle Communications Cloud Native Core, Converged Policy (Policy)	23.1.6	23.1.2	Policy 23.1.6 supports fresh installation and upgrade from 22.3.x, 22.4.x, and 23.1.x to 23.1.6. For more information, see *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Converged Policy (Policy)	23.1.5	23.1.2	Policy 23.1.5 supports fresh installation and upgrade from 22.3.x, 22.4.x, and 23.1.x to 23.1.5. For more information, see *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Converged Policy (Policy)	23.1.4	23.1.2	Policy 23.1.4 supports fresh installation and upgrade from 22.3.x, 22.4.x, and 23.1.x to 23.1.4. For more information, see *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide*.

Table 3-1 (Cont.) Media Pack Contents for Oracle Communications Cloud Native Core 2.23.1

Description	NF Version	ATS Version	Upgrade Supported
Oracle Communications Cloud Native Core, Converged Policy (Policy)	23.1.3	23.1.2	Policy 23.1.3 supports fresh installation and upgrade from 22.3.x, 22.4.x, and 23.1.x to 23.1.3. For more information, see *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Converged Policy (Policy)	23.1.2	23.1.2	Policy 23.1.2 supports fresh installation and upgrade from 22.3.x, 22.4.x, and 23.1.x to 23.1.2. For more information, see *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Converged Policy (Policy)	23.1.1	23.1.1	Policy 23.1.1 supports fresh installation and upgrade from 22.3.x, 22.4.x and 23.1.0 to 23.1.1. For more information, see *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Converged Policy (Policy)	23.1.0	23.1.0	Policy 23.1.0 supports fresh installation and upgrade from 22.3.x and 22.4.x to 23.1.0. For more information, see *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Network Exposure Function (NEF)	23.1.4	23.1.4	NEF 23.1.4 supports fresh installation and upgrade from 22.3.2, 22.4.x, and 23.1.x to 23.1.4. For more information, see *Oracle Communications Cloud Native Core, Network Exposure Function Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Network Exposure Function (NEF)	23.1.3	23.1.3	NEF 23.1.3 supports fresh installation and upgrade from 22.3.2, 22.4.x, and 23.1.x to 23.1.3. For more information, see *Oracle Communications Cloud Native Core, Network Exposure Function Installation, Upgrade, and Fault Recovery Guide*.

Table 3-1 (Cont.) Media Pack Contents for Oracle Communications Cloud Native Core 2.23.1

Description	NF Version	ATS Version	Upgrade Supported
Oracle Communications Cloud Native Core, Network Exposure Function (NEF)	23.1.2	23.1.1	NEF 23.1.2 supports fresh installation and upgrade from 22.3.2, 22.4.x, and 23.1.x to 23.1.2. For more information, see *Oracle Communications Cloud Native Core, Network Exposure Function Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Network Exposure Function (NEF)	23.1.1	23.1.1	NEF 23.1.1 supports fresh installation and upgrade from 22.3.2, 22.4.x, and 23.1.0 to 23.1.1. For more information, see *Oracle Communications Cloud Native Core, Network Exposure Function Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Network Exposure Function (NEF)	23.1.0	23.1.0	NEF 23.1.0 supports fresh installation and upgrade from 22.3.2 and 22.4.x to 23.1.0. For more information, see *Oracle Communications Cloud Native Core, Network Exposure Function Installation, Upgrade, and Fault Recovery Guide.*
Oracle Communications Cloud Native Core, Network Repository Function (NRF)	23.1.4	23.1.4	NRF 23.1.4 supports fresh installation and upgrade from 22.4.x and 23.1.x to 23.1.4. For more information, see *Oracle Communications Cloud Native Core Network Repository Function Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Network Repository Function (NRF)	23.1.3	23.1.3	NRF 23.1.3 supports fresh installation and upgrade from 22.4.x and 23.1.x to 23.1.3. For more information, see *Oracle Communications Cloud Native Core Network Repository Function Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Network Repository Function (NRF)	23.1.2	23.1.2	NRF 23.1.2 supports fresh installation and upgrade from 22.4.x and 23.1.x to 23.1.2. For more information, see *Oracle Communications Cloud Native Core Network Repository Function Installation, Upgrade, and Fault Recovery Guide*.

Table 3-1 (Cont.) Media Pack Contents for Oracle Communications Cloud Native Core 2.23.1

Description	NF Version	ATS Version	Upgrade Supported
Oracle Communications Cloud Native Core, Network Repository Function (NRF)	23.1.1	23.1.1	NRF 23.1.1 supports fresh installation and upgrade from 22.4.x and 23.1.0 to 23.1.1. For more information, see *Oracle Communications Cloud Native Core, Network Repository Function Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Network Repository Function (NRF)	23.1.0	23.1.0	NRF 23.1.0 supports fresh installation and upgrade from 22.4.x to 23.1.0. For more information, see *Oracle Communications Cloud Native Core, Network Repository Function Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Network Slice Selection Function (NSSF)	23.1.2	23.1.2	NSSF 23.1.2 supports fresh installation and upgrade from 23.1.0 and 23.1.1 to 23.1.2. For more information on installation, see *Oracle Communications Cloud Native Core, Network Slice Selection Function Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Network Slice Selection Function (NSSF)	23.1.1	23.1.1	NSSF 23.1.1 supports fresh installation and upgrade from 23.1.0 to 23.1.1. For more information, see *Oracle Communications Cloud Native Core, Network Slice Selection Function Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Network Slice Selection Function (NSSF)	23.1.0	23.1.0	NSSF 23.1.0 supports only fresh installation. For more information, see *Oracle Communications Cloud Native Core, Network Slice Selection Function Installation, Upgrade, and Fault Recovery Guide*. Note: A workaround procedure or MOP can be provided to enable an out of service rolling upgrade. For more information or to request the MOP, contact OCC or MOS.
Oracle Communications Cloud Native Core, Service Communications Proxy (SCP)	23.1.3	23.1.3	SCP 23.1.3 supports fresh installation and upgrade from 22.3.x, 22.4.x, and 23.1.x to 23.1.3. For more information, see *Oracle Communications Cloud Native Core, Service Communication Proxy Installation, Upgrade, and Fault Recovery Guide*.

Table 3-1 (Cont.) Media Pack Contents for Oracle Communications Cloud Native Core 2.23.1

Description	NF Version	ATS Version	Upgrade Supported
Oracle Communications Cloud Native Core, Service Communications Proxy (SCP)	23.1.2	23.1.2	SCP 23.1.2 supports fresh installation and upgrade from 22.3.x, 22.4.x, and 23.1.x to 23.1.2. For more information, see *Oracle Communications Cloud Native Core, Service Communication Proxy Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Service Communications Proxy (SCP)	23.1.1	23.1.1	SCP 23.1.1 supports fresh installation and upgrade from 22.3.x, 22.4.x, and 23.1.0 to 23.1.1. For more information, see *Oracle Communications Cloud Native Core, Service Communication Proxy Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Service Communications Proxy (SCP)	23.1.0	23.1.0	SCP 23.1.0 supports fresh installation and upgrade from 22.3.x and 22.4.x to 23.1.0. For more information, see *Oracle Communications Cloud Native Core, Service Communication Proxy Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Security Edge Protection Proxy (SEPP)	23.1.4	23.1.4	SEPP 23.1.4 supports fresh installation and upgrade from 22.3.x, 22.4.2, 22.4.3, and 23.1.x to 23.1.4. Roaming Hub mode supports the fresh installation and upgrade from 22.3.x, 22.4.2, 22.4.3, and 23.1.x to 23.1.4. For more information, see *Oracle Communications Cloud Native Core, Security Edge Protection Proxy Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Security Edge Protection Proxy (SEPP)	23.1.3	23.1.3	SEPP 23.1.3 supports fresh installation and upgrade from 22.3.x, 22.4.2, 22.4.3, and 23.1.x to 23.1.3. Roaming Hub mode supports the fresh installation and upgrade from 22.3.x, 22.4.2, 22.4.3, and 23.1.x to 23.1.3. For more information, see *Oracle Communications Cloud Native Core, Security Edge Protection Proxy Installation, Upgrade, and Fault Recovery Guide*.

Table 3-1 (Cont.) Media Pack Contents for Oracle Communications Cloud Native Core 2.23.1

Description	NF Version	ATS Version	Upgrade Supported
Oracle Communications Cloud Native Core, Security Edge Protection Proxy (SEPP)	23.1.2	23.1.3	SEPP 23.1.2 supports fresh installation and upgrade from 22.3.x, 22.4.2, 22.4.3, and 23.1.x to 23.1.2. Roaming Hub mode supports the fresh installation and upgrade from 22.3.x, 22.4.2, 22.4.3, and 23.1.x to 23.1.2. For more information, see *Oracle Communications Cloud Native Core, Security Edge Protection Proxy Installation, Upgrade, and Fault Recovery Guide.*
Oracle Communications Cloud Native Core, Security Edge Protection Proxy (SEPP)	23.1.1	23.1.1	SEPP 23.1.1 supports fresh installation and upgrade from 22.3.x, 22.4.2, 22.4.3, and 23.1.0 to 23.1.1. Roaming Hub mode supports the fresh installation and upgrade from 22.3.x, 22.4.2, 22.4.3, and 23.1.0 to 23.1.1. For more information, see *Oracle Communications Cloud Native Core, Security Edge Protection Proxy Installation, Upgrade, and Fault Recovery Guide.*
Oracle Communications Cloud Native Core, Security Edge Protection Proxy (SEPP)	23.1.0	23.1.0	SEPP 23.1.0 supports fresh installation and upgrade from 22.3.x and 22.4.2 to 23.1.0. Roaming Hub mode supports the fresh installation and upgrade from 22.3.x and 22.4.2 to 23.1.0. For more information, see *Oracle Communications Cloud Native Core, Security Edge Protection Proxy Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Unified Data Repository (UDR)	23.1.3	23.1.3	UDR 23.1.3 supports fresh installation and upgrade from 22.4.x and 23.1.x to 23.1.3. For more information on installation or upgrading, see *Oracle Communications Cloud Native Core, Unified Data Repository Installation, Upgrade, and Fault Recovery Guide.*
Oracle Communications Cloud Native Core, Unified Data Repository (UDR)	23.1.2	23.1.2	UDR 23.1.2 supports fresh installation and upgrade from 22.4.x and 23.1.x to 23.1.2. For more information on installation or upgrading, see *Oracle Communications Cloud Native Core, Unified Data Repository Installation, Upgrade, and Fault Recovery Guide.*

Table 3-1 (Cont.) Media Pack Contents for Oracle Communications Cloud Native Core 2.23.1

Description	NF Version	ATS Version	Upgrade Supported
Oracle Communications Cloud Native Core, Unified Data Repository (UDR)	23.1.1	23.1.1	UDR 23.1.1 supports fresh installation and upgrade from 22.2.x, 22.3.x, 22.4.x, and 23.1.0 to 23.1.1. For more information, see *Oracle Communications Cloud Native Core, Unified Data Repository Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Unified Data Repository (UDR)	23.1.0	23.1.0	UDR 23.1.0 supports fresh installation and upgrade from 22.2.x, 22.3.x, and 22.4.x to 23.1.0. For more information, see *Oracle Communications Cloud Native Core, Unified Data Repository Installation, Upgrade, and Fault Recovery Guide*.

3.2 Compatibility Matrix

The following table lists the compatibility matrix for each network function:

Table 3-2 Compatibility Matrix

CNC NF	NF Version	CNE	cnDBTier	CDCS	OSO	Kubernetes	CNC Console	3GPP
BSF	23.1.4	• 23.1.x • 22.4.x • 22.3.x	• 23.1.x • 22.4.x • 22.3.x	NA	• 22.3.x • 1.10.x • 1.6.x	• 1.24.x • 1.23.x • 1.22.x	23.1.x	• 3GPP TS 23.501 • 3GPP TS 23.502 • 3GPP TS 23.503 • 3GPP TS 29.500 • 3GPP TS 29.504 • 3GPP TS 29.510 • 3GPP TS 29.514 • 3GPP TS 29.521 • 3GPP TS 29.214
BSF	23.1.3	• 23.1.x • 22.4.x • 22.3.x	• 23.1.x • 22.4.x • 22.3.x	NA	• 22.3.x • 1.10.x • 1.6.x	• 1.24.x • 1.23.x • 1.22.x	23.1.x	• 3GPP TS 23.501 • 3GPP TS 23.502 • 3GPP TS 23.503 • 3GPP TS 29.500 • 3GPP TS 29.504 • 3GPP TS 29.510 • 3GPP TS 29.514 • 3GPP TS 29.521 • 3GPP TS 29.214

Table 3-2 (Cont.) Compatibility Matrix

CNC NF	NF Version	CNE	cnDBTier	CDCS	OSO	Kubernetes	CNC Console	3GPP
BSF	23.1.2	• 23.1.x • 22.4.x • 22.3.x	• 23.1.x • 22.4.x • 22.3.x	NA	• 22.3.x • 1.10.x • 1.6.x	• 1.24.x • 1.23.x • 1.22.x	23.1.x	• 3GPP TS 23.501 • 3GPP TS 23.502 • 3GPP TS 23.503 • 3GPP TS 29.500 • 3GPP TS 29.504 • 3GPP TS 29.510 • 3GPP TS 29.514 • 3GPP TS 29.521 • 3GPP TS 29.214
BSF	23.1.1	• 23.1.x • 22.4.x • 22.3.x	• 23.1.x • 22.4.x • 22.3.x	NA	• 22.3.x • 1.10.x • 1.6.x	• 1.24.x • 1.23.x • 1.22.x	23.1.x	• 3GPP TS 23.501 • 3GPP TS 23.502 • 3GPP TS 23.503 • 3GPP TS 29.500 • 3GPP TS 29.504 • 3GPP TS 29.510 • 3GPP TS 29.514 • 3GPP TS 29.521 • 3GPP TS 29.214
BSF	23.1.0	• 23.1.x • 22.4.x • 22.3.x	• 23.1.x • 22.4.x • 22.3.x	NA	• 22.3.x • 1.10.x • 1.6.x	• 1.24.x • 1.23.x • 1.22.x	23.1.x	• 3GPP TS 23.501 • 3GPP TS 23.502 • 3GPP TS 23.503 • 3GPP TS 29.500 • 3GPP TS 29.504 • 3GPP TS 29.510 • 3GPP TS 29.514 • 3GPP TS 29.521 • 3GPP TS 29.214
CDCS	23.1.1	• 22.4.x • 22.3.x • 22.2.x	NA	NA	NA	NA	NA	NA
CDCS	23.1.0	• 22.4.x • 22.3.x • 22.2.x	NA	NA	NA	NA	NA	NA
CNC Console	23.1.3	• 23.1.x • 22.4.x • 22.3.x	• 23.1.x • 22.4.x • 22.3.x	• 23.1.x • 22.4.x • 22.3.x	• 22.3.x • 1.10.x • 1.6.x	• 1.24.x • 1.23.x • 1.22.x	NA	NA

Table 3-2 (Cont.) Compatibility Matrix

CNC NF	NF Version	CNE	cnDBTier	CDCS	OSO	Kubernetes	CNC Console	3GPP
CNC Console	23.1.2	• 23.1.x • 22.4.x • 22.3.x	• 23.1.x • 22.4.x • 22.3.x	• 23.1.x • 22.4.x • 22.3.x	• 22.3.x • 1.10.x • 1.6.x	• 1.24.x • 1.23.x • 1.22.x	NA	NA
CNC Console	23.1.1	• 23.1.x • 22.4.x • 22.3.x	• 23.1.x • 22.4.x • 22.3.x	• 23.1.x • 22.4.x • 22.3.x	• 22.3.x • 1.10.x • 1.6.x	• 1.24.x • 1.23.x • 1.22.x	NA	NA
CNC Console	23.1.0	• 23.1.x • 22.4.x • 22.3.x	• 23.1.x • 22.4.x • 22.3.x	• 23.1.x • 22.4.x • 22.3.x	• 22.3.x • 1.10.x • 1.6.x	• 1.24.x • 1.23.x • 1.22.x	NA	NA
CNE	23.1.4	NA	NA	NA	NA	1.24.x	NA	NA
CNE	23.1.3	NA	NA	NA	NA	1.24.x	NA	NA
CNE	23.1.2	NA	NA	NA	NA	1.24.x	NA	NA
CNE	23.1.1	NA	NA	NA	NA	1.24.x	NA	NA
CNE	23.1.0	NA	NA	NA	NA	1.24.x	NA	NA
cnDBTier	23.1.3	• 23.1.x • 22.4.x • 22.3.x • 22.2.x • 22.1.x	NA	NA	NA	• 1.24.x • 1.23.x • 1.22.x • 1.21.x	NA	NA
cnDBTier	23.1.2	• 23.1.x • 22.4.x • 22.3.x • 22.2.x • 22.1.x	NA	NA	NA	• 1.24.x • 1.23.x • 1.22.x • 1.21.x	NA	NA
cnDBTier	23.1.1	• 23.1.x • 22.4.x • 22.3.x • 22.2.x • 22.1.x	NA	NA	NA	• 1.24.x • 1.23.x • 1.22.x • 1.21.x	NA	NA

Table 3-2 (Cont.) Compatibility Matrix

CNC NF	NF Version	CNE	cnDBTier	CDCS	OSO	Kubernetes	CNC Console	3GPP
cnDBTier	23.1.0	• 23.1.x • 22.4.x • 22.3.x • 22.2.x • 22.1.x	NA	NA	NA	• 1.24.x • 1.23.x • 1.22.x • 1.21.x	NA	NA
NEF	23.1.4	• 23.1.x • 22.4.x • 22.3.x	• 23.1.x • 22.4.x • 22.3.x	NA	NA	• 1.24.x • 1.23.x • 1.22.x	NA	• 3GPP TS 29.122 v16.10.0 • 3GPP TS 23.222 v16.9.0 • 3GPP TS 23.501 v 16.10.0 • 3GPP TS 23.502 v 16.10.0 • 3GPP TS 29.514 v16.10.0 • 3GPP TS 29.521 v16.10 • 3GPP TS 29.503 v16.10 • 3GPP TS 29.515 v16.7 • 3GPP TS 29.222 v16.5.0 • 3GPP TS 29.500 v16.6.0 • 3GPP TS29.501 v16.6.0 • 3GPP TS 29.522 v16.10 • 3GPP TS29.510 v16.6.0 • 3GPP TS 29.591 v16.3.0 • 3GPP TS 29.518 v16.6.0 • 3GPP TS 33.501 v17.7.0 • 3GPP TS 29.504 v16.10.0 • 3GPP TS 29.519 v16.11.0 • 3GPP TS 29508 v16.10.0

Table 3-2 (Cont.) Compatibility Matrix

CNC NF	NF Version	CNE	cnDBTier	CDCS	OSO	Kubernetes	CNC Console	3GPP
NEF	23.1.3	• 23.1.x • 22.4.x • 22.3.x	• 23.1.x • 22.4.x • 22.3.x	NA	NA	• 1.24.x • 1.23.x • 1.22.x	NA	• 3GPP TS 29.122 v16.10.0 • 3GPP TS 23.222 v16.9.0 • 3GPP TS 23.501 v 16.10.0 • 3GPP TS 23.502 v 16.10.0 • 3GPP TS 29.514 v16.10.0 • 3GPP TS 29.521 v16.10 • 3GPP TS 29.503 v16.10 • 3GPP TS 29.515 v16.7 • 3GPP TS 29.222 v16.5.0 • 3GPP TS 29.500 v16.6.0 • 3GPP TS29.501 v16.6.0 • 3GPP TS 29.522 v16.10 • 3GPP TS29.510 v16.6.0 • 3GPP TS 29.591 v16.3.0 • 3GPP TS 29.518 v16.6.0 • 3GPP TS 33.501 v17.7.0 • 3GPP TS 29.504 v16.10.0 • 3GPP TS 29.519 v16.11.0 • 3GPP TS 29508 v16.10.0

Table 3-2 (Cont.) Compatibility Matrix

CNC NF	NF Version	CNE	cnDBTier	CDCS	OSO	Kubernetes	CNC Console	3GPP
NEF	23.1.2	• 23.1.x • 22.4.x • 22.3.x	• 23.1.x • 22.4.x • 22.3.x	NA	NA	• 1.24.x • 1.23.x • 1.22.x	NA	• 3GPP TS 29.122 v16.10.0 • 3GPP TS 23.222 v16.9.0 • 3GPP TS 23.501 v 16.10.0 • 3GPP TS 23.502 v 16.10.0 • 3GPP TS 29.514 v16.10.0 • 3GPP TS 29.521 v16.10 • 3GPP TS 29.503 v16.10 • 3GPP TS 29.515 v16.7 • 3GPP TS 29.222 v16.5.0 • 3GPP TS 29.500 v16.6.0 • 3GPP TS29.501 v16.6.0 • 3GPP TS 29.522 v16.10 • 3GPP TS29.510 v16.6.0 • 3GPP TS 29.591 v16.3.0 • 3GPP TS 29.518 v16.6.0 • 3GPP TS 33.501 v17.7.0 • 3GPP TS 29.504 v16.10.0 • 3GPP TS 29.519 v16.11.0 • 3GPP TS 29508 v16.10.0

Table 3-2 (Cont.) Compatibility Matrix

CNC NF	NF Version	CNE	cnDBTier	CDCS	OSO	Kubernetes	CNC Console	3GPP
NEF	23.1.1	• 23.1.x • 22.4.x • 22.3.x	• 23.1.x • 22.4.x • 22.3.x	NA	NA	• 1.24.x • 1.23.x • 1.22.x	NA	• 3GPP TS 29.122 v16.10.0 • 3GPP TS 23.222 v16.9.0 • 3GPP TS 23.501 v 16.10.0 • 3GPP TS 23.502 v 16.10.0 • 3GPP TS 29.514 v16.10.0 • 3GPP TS 29.521 v16.10 • 3GPP TS 29.503 v16.10 • 3GPP TS 29.515 v16.7 • 3GPP TS 29.222 v16.5.0 • 3GPP TS 29.500 v16.6.0 • 3GPP TS29.501 v16.6.0 • 3GPP TS 29.522 v16.10 • 3GPP TS29.510 v16.6.0 • 3GPP TS 29.591 v16.3.0 • 3GPP TS 29.518 v16.6.0 • 3GPP TS 33.501 v17.7.0 • 3GPP TS 29.504 v16.10.0 • 3GPP TS 29.519 v16.11.0 • 3GPP TS 29508 v16.10.0

Table 3-2 (Cont.) Compatibility Matrix

CNC NF	NF Version	CNE	cnDBTier	CDCS	OSO	Kubernetes	CNC Console	3GPP
NEF	23.1.0	• 23.1.x • 22.4.x • 22.3.x	• 23.1.x • 22.4.x • 22.3.x	NA	NA	• 1.24.x • 1.23.x • 1.22.x	NA	• 3GPP TS 29.122 v16.10.0 • 3GPP TS 23.222 v16.9.0 • 3GPP TS 23.501 v 16.10.0 • 3GPP TS 23.502 v 16.10.0 • 3GPP TS 29.514 v16.10.0 • 3GPP TS 29.521 v16.10 • 3GPP TS 29.503 v16.10 • 3GPP TS 29.515 v16.7 • 3GPP TS 29.222 v16.5.0 • 3GPP TS 29.500 v16.6.0 • 3GPP TS29.501 v16.6.0 • 3GPP TS 29.522 v16.10 • 3GPP TS29.510 v16.6.0 • 3GPP TS 29.591 v16.3.0 • 3GPP TS 29.518 v16.6.0 • 3GPP TS 33.501 v17.7.0 • 3GPP TS 29.504 v16.10.0 • 3GPP TS 29.519 v16.11.0 • 3GPP TS 29508 v16.10.0
NRF	23.1.4	• 23.1.x • 22.4.x • 22.3.x	• 23.1.x • 22.4.x • 22.3.x	NA	• 22.3.x • 1.10.x • 1.6.x	• 1.24.x • 1.23.x • 1.22.x	23.1.x	• 3GPP TS 29.510 v15.5 • 3GPP TS 29.510 v16.3.0 • 3GPP TS 29.510 v16.7
NRF	23.1.2	• 23.1.x • 22.4.x • 22.3.x	• 23.1.x • 22.4.x • 22.3.x	NA	• 22.3.x • 1.10.x • 1.6.x	• 1.24.x • 1.23.x • 1.22.x	23.1.x	• 3GPP TS 29.510 v15.5 • 3GPP TS 29.510 v16.3.0 • 3GPP TS 29.510 v16.7

Table 3-2 (Cont.) Compatibility Matrix

CNC NF	NF Version	CNE	cnDBTier	CDCS	OSO	Kubernetes	CNC Console	3GPP
NRF	23.1.1	• 23.1.x • 22.4.x • 22.3.x	• 23.1.x • 22.4.x • 22.3.x	NA	• 22.3.x • 1.10.x • 1.6.x	• 1.24.x • 1.23.x • 1.22.x	23.1.x	• 3GPP TS 29.510 v15.5 • 3GPP TS 29.510 v16.3.0 • 3GPP TS 29.510 v16.7
NRF	23.1.0	• 23.1.x • 22.4.x • 22.3.x	• 23.1.x • 22.4.x • 22.3.x	NA	• 22.3.x • 1.10.x • 1.6.x	• 1.24.x • 1.23.x • 1.22.x	23.1.x	• 3GPP TS 29.510 v15.5 • 3GPP TS 29.510 v16.3.0 • 3GPP TS 29.510 v16.7
NSSF	23.1.2	• 23.1.x • 22.4.x • 22.3.x	• 23.1.x • 22.4.x • 22.3.x	NA	• 22.3.x • 1.10.x • 1.6.x	• 1.24.x • 1.23.x • 1.22.x	23.1.x	• 3GPP TS 29.531 v15.5.0 • 3GPP TS 29.531 v16.5.0
NSSF	23.1.1	• 23.1.x • 22.4.x • 22.3.x	• 23.1.x • 22.4.x • 22.3.x	NA	• 22.3.x • 1.10.x • 1.6.x	• 1.24.x • 1.23.x • 1.22.x	23.1.x	• 3GPP TS 29.531 v15.5.0 • 3GPP TS 29.531 v16.5.0
NSSF	23.1.0	• 23.1.x • 22.4.x • 22.3.x	• 23.1.x • 22.4.x • 22.3.x	NA	• 22.3.x • 1.10.x • 1.6.x	• 1.24.x • 1.23.x • 1.22.x	23.1.x	• 3GPP TS 29.531 v15.5.0 • 3GPP TS 29.531 v16.5.0
Policy	23.1.8	• 23.1.x • 22.4.x • 22.3.x	• 23.1.x • 22.4.x • 22.3.x	NA	• 22.3.x • 1.10.x • 1.6.x	• 1.24.x • 1.23.x • 1.22.x	23.1.x	• 3GPP TS 23.501 • 3GPP TS 23.502 • 3GPP TS 23.503 • 3GPP TS 29.500 • 3GPP TS 29.504 • 3GPP TS 29.510 • 3GPP TS 29.507 • 3GPP TS 29.512 • 3GPP TS 29.513 • 3GPP TS 29.514 • 3GPP TS 29.519 • 3GPP TS 29.521 • 3GPP TS 29.525 • 3GPP TS 29.594 • 3GPP TS 29.214 • 3GPP TS 29.212

Table 3-2 (Cont.) Compatibility Matrix

CNC NF	NF Version	CNE	cnDBTier	CDCS	OSO	Kubernetes	CNC Console	3GPP
Policy	23.1.7	• 23.1.x • 22.4.x • 22.3.x	• 23.1.x • 22.4.x • 22.3.x	NA	• 22.3.x • 1.10.x • 1.6.x	• 1.24.x • 1.23.x • 1.22.x	23.1.x	• 3GPP TS 23.501 • 3GPP TS 23.502 • 3GPP TS 23.503 • 3GPP TS 29.500 • 3GPP TS 29.504 • 3GPP TS 29.510 • 3GPP TS 29.507 • 3GPP TS 29.512 • 3GPP TS 29.513 • 3GPP TS 29.514 • 3GPP TS 29.519 • 3GPP TS 29.521 • 3GPP TS 29.525 • 3GPP TS 29.594 • 3GPP TS 29.214 • 3GPP TS 29.212
Policy	23.1.6	• 23.1.x • 22.4.x • 22.3.x	• 23.1.x • 22.4.x • 22.3.x	NA	• 22.3.x • 1.10.x • 1.6.x	• 1.24.x • 1.23.x • 1.22.x	23.1.x	• 3GPP TS 23.501 • 3GPP TS 23.502 • 3GPP TS 23.503 • 3GPP TS 29.500 • 3GPP TS 29.504 • 3GPP TS 29.510 • 3GPP TS 29.507 • 3GPP TS 29.512 • 3GPP TS 29.513 • 3GPP TS 29.514 • 3GPP TS 29.519 • 3GPP TS 29.521 • 3GPP TS 29.525 • 3GPP TS 29.594 • 3GPP TS 29.214 • 3GPP TS 29.212
Policy	23.1.5	• 23.1.x • 22.4.x • 22.3.x	• 23.1.x • 22.4.x • 22.3.x	NA	• 22.3.x • 1.10.x • 1.6.x	• 1.24.x • 1.23.x • 1.22.x	23.1.x	• 3GPP TS 23.501 • 3GPP TS 23.502 • 3GPP TS 23.503 • 3GPP TS 29.500 • 3GPP TS 29.504 • 3GPP TS 29.510 • 3GPP TS 29.507 • 3GPP TS 29.512 • 3GPP TS 29.513 • 3GPP TS 29.514 • 3GPP TS 29.519 • 3GPP TS 29.521 • 3GPP TS 29.525 • 3GPP TS 29.594 • 3GPP TS 29.214 • 3GPP TS 29.212

Table 3-2 (Cont.) Compatibility Matrix

CNC NF	NF Version	CNE	cnDBTier	CDCS	OSO	Kubernetes	CNC Console	3GPP
Policy	23.1.4	• 23.1.x • 22.4.x • 22.3.x	• 23.1.x • 22.4.x • 22.3.x	NA	• 22.3.x • 1.10.x • 1.6.x	• 1.24.x • 1.23.x • 1.22.x	23.1.x	• 3GPP TS 23.501 • 3GPP TS 23.502 • 3GPP TS 23.503 • 3GPP TS 29.500 • 3GPP TS 29.504 • 3GPP TS 29.510 • 3GPP TS 29.507 • 3GPP TS 29.512 • 3GPP TS 29.513 • 3GPP TS 29.514 • 3GPP TS 29.519 • 3GPP TS 29.521 • 3GPP TS 29.525 • 3GPP TS 29.594 • 3GPP TS 29.214 • 3GPP TS 29.212
Policy	23.1.2	• 23.1.x • 22.4.x • 22.3.x	• 23.1.x • 22.4.x • 22.3.x	NA	• 22.3.x • 1.10.x • 1.6.x	• 1.24.x • 1.23.x • 1.22.x	23.1.x	• 3GPP TS 23.501 • 3GPP TS 23.502 • 3GPP TS 23.503 • 3GPP TS 29.500 • 3GPP TS 29.504 • 3GPP TS 29.510 • 3GPP TS 29.507 • 3GPP TS 29.512 • 3GPP TS 29.513 • 3GPP TS 29.514 • 3GPP TS 29.519 • 3GPP TS 29.521 • 3GPP TS 29.525 • 3GPP TS 29.594 • 3GPP TS 29.214 • 3GPP TS 29.212
Policy	23.1.1	• 23.1.x • 22.4.x • 22.3.x	• 23.1.x • 22.4.x • 22.3.x	NA	• 22.3.x • 1.10.x • 1.6.x	• 1.24.x • 1.23.x • 1.22.x	23.1.x	• 3GPP TS 23.501 • 3GPP TS 23.502 • 3GPP TS 23.503 • 3GPP TS 29.500 • 3GPP TS 29.504 • 3GPP TS 29.510 • 3GPP TS 29.507 • 3GPP TS 29.512 • 3GPP TS 29.513 • 3GPP TS 29.514 • 3GPP TS 29.519 • 3GPP TS 29.521 • 3GPP TS 29.525 • 3GPP TS 29.594 • 3GPP TS 29.214 • 3GPP TS 29.212

Table 3-2 (Cont.) Compatibility Matrix

CNC NF	NF Version	CNE	cnDBTier	CDCS	OSO	Kubernetes	CNC Console	3GPP
Policy	23.1.0	• 23.1.x • 22.4.x • 22.3.x	• 23.1.x • 22.4.x • 22.3.x	NA	• 22.3.x • 1.10.x • 1.6.x	• 1.24.x • 1.23.x • 1.22.x	23.1.x	• 3GPP TS 23.501 • 3GPP TS 23.502 • 3GPP TS 23.503 • 3GPP TS 29.500 • 3GPP TS 29.504 • 3GPP TS 29.510 • 3GPP TS 29.507 • 3GPP TS 29.512 • 3GPP TS 29.513 • 3GPP TS 29.514 • 3GPP TS 29.519 • 3GPP TS 29.521 • 3GPP TS 29.525 • 3GPP TS 29.594 • 3GPP TS 29.214 • 3GPP TS 29.212
SCP	23.1.3	• 23.1.x • 22.4.x • 22.3.x	• 23.1.x • 22.4.x • 22.3.x	• 23.1.x • 22.4.x • 22.3.x	• 22.3.x • 1.10.x • 1.6.x	• 1.24.x • 1.23.x • 1.22.x	23.1.x	• 3GPP TS 29.500 v 16.6.0 • 3GPP TS 29.501 v 16.5.0 • 3GPP TS 29.510 v 16.6.0
SCP	23.1.2	• 23.1.x • 22.4.x • 22.3.x	• 23.1.x • 22.4.x • 22.3.x	• 23.1.x • 22.4.x • 22.3.x	• 22.3.x • 1.10.x • 1.6.x	• 1.24.x • 1.23.x • 1.22.x	23.1.x	• 3GPP TS 29.500 v 16.6.0 • 3GPP TS 29.501 v 16.5.0 • 3GPP TS 29.510 v 16.6.0
SCP	23.1.1	• 23.1.x • 22.4.x • 22.3.x	• 23.1.x • 22.4.x • 22.3.x	• 23.1.x • 22.4.x • 22.3.x	• 22.3.x • 1.10.x • 1.6.x	• 1.24.x • 1.23.x • 1.22.x	23.1.x	• 3GPP TS 29.500 v 16.6.0 • 3GPP TS 29.501 v 16.5.0 • 3GPP TS 29.510 v 16.6.0

Table 3-2 (Cont.) Compatibility Matrix

CNC NF	NF Version	CNE	cnDBTier	CDCS	OSO	Kubernetes	CNC Console	3GPP
SCP	23.1.0	• 23.1.x • 22.4.x • 22.3.x	• 23.1.x • 22.4.x • 22.3.x	• 23.1.x • 22.4.x • 22.3.x	• 22.3.x • 1.10.x • 1.6.x	• 1.24.x • 1.23.x • 1.22.x	23.1.x	• 3GPP TS 29.500 v16.6.0 • 3GPP TS 29.501 v16.5.0 • 3GPP TS 29.510 v16.6.0
SEPP	23.1.4	• 23.1.x • 22.4.x • 22.3.x	• 23.1.x • 22.4.x • 22.3.x	• 23.1.x • 22.4.x • 22.3.x	22.3.x	• 1.24.x • 1.23.x • 1.22.x	23.1.x	• 3GPP TS 23.501 v17.6.0 • 3GPP TS 23.502 v17.6.0 • 3GPP TS 29.500 v17.8.0 • 3GPP TS 29.501 v17.7.0 • 3GPP TS 29.510 v17.7.0 • 3GPP TS 33.501 v17.7.0 • 3GPP TS 33.117 v17.1.0 • 3GPP TS 33.210 v17.1.0
SEPP	23.1.3	• 23.1.x • 22.4.x • 22.3.x	• 23.1.x • 22.4.x • 22.3.x	• 23.1.x • 22.4.x • 22.3.x	22.3.x	• 1.24.x • 1.23.x • 1.22.x	23.1.x	• 3GPP TS 23.501 v17.6.0 • 3GPP TS 23.502 v17.6.0 • 3GPP TS 29.500 v17.8.0 • 3GPP TS 29.501 v17.7.0 • 3GPP TS 29.510 v17.7.0 • 3GPP TS 33.501 v17.7.0 • 3GPP TS 33.117 v17.1.0 • 3GPP TS 33.210 v17.1.0

Table 3-2 (Cont.) Compatibility Matrix

CNC NF	NF Version	CNE	cnDBTier	CDCS	OSO	Kubernetes	CNC Console	3GPP
SEPP	23.1.2	• 23.1.x • 22.4.x • 22.3.x	• 23.1.x • 22.4.x • 22.3.x	• 23.1.x • 22.4.x • 22.3.x	22.3.x	• 1.24.x • 1.23.x • 1.22.x	23.1.x	• 3GPP TS 23.501 v16.7.0 • 3GPP TS 23.502 v16.7.0 • 3GPP TS 29.500 v16.6.0 • 3GPP TS 29.501 v16.5.0 • 3GPP TS 29.510 v16.6.0 • 3GPP TS 29.573 v16.3.0
SEPP	23.1.1	• 23.1.x • 22.4.x • 22.3.x	• 23.1.x • 22.4.x • 22.3.x	• 23.1.x • 22.4.x • 22.3.x	22.3.x	• 1.24.x • 1.23.x • 1.22.x	23.1.x	• 3GPP TS 23.501 v16.7.0 • 3GPP TS 23.502 v16.7.0 • 3GPP TS 29.500 v16.6.0 • 3GPP TS 29.501 v16.5.0 • 3GPP TS 29.510 v16.6.0 • 3GPP TS 29.573 v16.3.0
SEPP	23.1.0	• 23.1.x • 22.4.x • 22.3.x	• 23.1.x • 22.4.x • 22.3.x	• 23.1.x • 22.4.x • 22.3.x	22.3.x	• 1.24.x • 1.23.x • 1.22.x	23.1.x	• 3GPP TS 23.501 v16.7.0 • 3GPP TS 23.502 v16.7.0 • 3GPP TS 29.500 v16.6.0 • 3GPP TS 29.501 v16.5.0 • 3GPP TS 29.510 v16.6.0 • 3GPP TS 29.573 v16.3.0
UDR	23.1.3	• 23.1.x • 22.4.x • 22.3.x	• 23.1.x • 22.4.x • 22.3.x	NA	• 22.3.x • 1.10.x • 1.6.x	• 1.24.x • 1.23.x • 1.22.x	23.1.x	• 3GPP TS 29.505 v15.4.0 • 3GPP TS 29.504 v16.2.0 • 3GPP TS 29.519 v16.2.0 • 3GPP TS 29.511 v17.2.0

Table 3-2 (Cont.) Compatibility Matrix

CNC NF	NF Version	CNE	cnDBTier	CDCS	OSO	Kubernetes	CNC Console	3GPP
UDR	23.1.2	• 23.1.x • 22.4.x • 22.3.x	• 23.1.x • 22.4.x • 22.3.x	NA	• 22.3.x • 1.10.x • 1.6.x	• 1.24.x • 1.23.x • 1.22.x	23.1.x	• 3GPP TS 29.505 v15.4.0 • 3GPP TS 29.504 v16.2.0 • 3GPP TS 29.519 v16.2.0 • 3GPP TS 29.511 v17.2.0
UDR	23.1.1	• 23.1.x • 22.4.x • 22.3.x	• 23.1.x • 22.4.x • 22.3.x	NA	• 22.3.x • 1.10.x • 1.6.x	• 1.24.x • 1.23.x • 1.22.x	23.1.x	• 3GPP TS 29.505 v15.4.0 • 3GPP TS 29.504 v16.2.0 • 3GPP TS 29.519 v16.2.0 • 3GPP TS 29.511 v17.2.0
UDR	23.1.0	• 23.1.x • 22.4.x • 22.3.x	• 23.1.x • 22.4.x • 22.3.x	NA	• 22.3.x • 1.10.x • 1.6.x	• 1.24.x • 1.23.x • 1.22.x	23.1.x	• 3GPP TS 29.505 v15.4.0 • 3GPP TS 29.504 v16.2.0 • 3GPP TS 29.519 v16.2.0 • 3GPP TS 29.511 v17.2.0

3.3 Common Microservices Load Lineup

This section provides information about common microservices and ATS for the specific NF versions in Oracle Communications Cloud Native Core Release 2.23.1.

Table 3-3 Common Microservices Load Lineup for Network Functions

CNC NF	NF Version	Alternate Route Svc	App-Info	ASM Configuration	ATS Framework	Config-Server	Debug-tool	Egress Gateway	Ingress Gateway	Helm Test	Mediation	NRF-Client	Perf-Info
BSF	23.1.4	23.1.12	23.1.8	23.1.4	23.1.4	23.1.8	23.1.3	23.1.12	23.1.12	23.1.3	NA	23.1.3	23.1.8
BSF	23.1.3	23.1.10	23.1.7	23.1.3	23.1.2	23.1.7	23.1.2	23.1.10	23.1.10	23.1.2	NA	23.1.2	23.1.7
BSF	23.1.2	23.1.4	23.1.3	23.1.3	23.1.1	23.1.3	23.1.0	23.1.4	23.1.4	23.1.1	NA	23.1.1	23.1.3
BSF	23.1.1	23.1.4	23.1.2	23.1.1	23.1.1	23.1.2	23.1.0	23.1.4	23.1.4	23.1.1	NA	23.1.1	23.1.2
BSF	23.1.0	23.1.3	23.1.0	23.1.0	23.1.0	23.1.0	23.1.0	23.1.3	23.1.3	23.1.0	NA	23.1.0	23.1.0
CNC Console	23.1.3	NA	NA	NA	NA	NA	23.1.3	NA	23.1.12	23.1.3	NA	NA	NA
CNC Console	23.1.2	NA	NA	NA	NA	NA	23.1.2	NA	23.1.10	23.1.2	NA	NA	NA

Table 3-3 (Cont.) Common Microservices Load Lineup for Network Functions

CNC NF	NF Version	Alternate Route Svc	App-Info	ASM Configuration	ATS Framework	Config-Server	Debug-tool	Egress Gateway	Ingress Gateway	Helm Test	Mediation	NRF-Client	Perf-Info
CNC Console	23.1.1	NA	NA	NA	NA	NA	23.1.0	NA	23.1.3	23.1.0	NA	NA	NA
CNC Console	23.1.0	NA	NA	NA	NA	NA	23.1.0	NA	23.1.3	23.1.0	NA	NA	NA
NEF	23.1.4	NA	23.1.8	NA	23.1.4	23.1.8	23.1.3	23.1.12	23.1.12	23.1.3	NA	23.1.3	23.1.8
NEF	23.1.3	NA	23.1.7	NA	23.1.3	23.1.7	23.1.2	23.1.9	23.1.9	23.1.2	NA	23.1.2	23.1.7
NEF	23.1.2	NA	23.1.2	NA	23.1.1	23.1.2	23.1.1	23.1.4	23.1.4	23.1.1	NA	23.1.1	23.1.2
NEF	23.1.1	NA	23.1.2	NA	23.1.1	23.1.2	23.1.1	23.1.4	23.1.4	23.1.1	NA	23.1.1	23.1.2
NEF	23.1.0	NA	23.1.0	NA	23.1.0	23.1.0	23.1.0	23.1.3	23.1.3	23.1.0	NA	23.1.0	23.1.0
NRF	23.1.4	23.1.12	23.1.8	23.1.0	23.1.4	NA	23.1.3	23.1.12	23.1.12	23.1.3	NA	NA	23.1.8
NRF	23.1.3	23.1.11	23.1.7	23.1.0	23.1.3	NA	23.1.2	23.1.11	23.1.11	23.1.2	NA	NA	23.1.7
NRF	23.1.2	23.1.8	23.1.7	23.1.0	23.1.2	NA	23.1.2	23.1.8	23.1.8	23.1.2	NA	NA	23.1.7
NRF	23.1.1	23.1.4	23.1.2	23.1.0	23.1.1	NA	23.1.1	23.1.4	23.1.4	23.1.1	NA	NA	23.1.2
NRF	23.1.0	23.1.3	23.1.0	23.1.0	23.1.0	NA	23.1.0	23.1.3	23.1.3	23.1.0	NA	23.1.0	23.1.0
NSSF	23.1.2	23.1.9	23.1.7	23.1.2	23.1.2	23.1.7	23.1.2	23.1.9	23.1.9	23.1.2	NA	23.1.2	23.1.7
NSSF	23.1.1	23.1.4	23.1.2	23.1.0	23.1.1	23.1.2	23.1.1	23.1.4	23.1.4	23.1.1	NA	23.1.1	23.1.2
NSSF	23.1.0	23.1.3	23.1.0	23.1.0	23.1.0	23.1.0	23.1.0	23.1.3	23.1.3	23.1.0	NA	23.1.0	23.1.0
Policy	23.1.8	23.1.12	23.1.8	23.1.8	23.1.2	23.1.8	23.1.3	23.1.12	23.1.12	23.1.3	NA	23.1.3	23.1.8
Policy	23.1.7	23.1.10	23.1.8	23.1.7	23.1.2	23.1.8	23.1.2	23.1.10	23.1.10	23.1.2	NA	23.1.2	23.1.8
Policy	23.1.6	23.1.4	23.1.3	23.1.3	23.1.1	23.1.3	23.1.0	23.1.4	23.1.4	23.1.1	NA	23.1.1	23.1.3
Policy	23.1.5	23.1.4	23.1.3	23.1.3	23.1.1	23.1.3	23.1.0	23.1.4	23.1.4	23.1.1	NA	23.1.1	23.1.3
Policy	23.1.4	23.1.4	23.1.3	23.1.3	23.1.1	23.1.3	23.1.0	23.1.4	23.1.4	23.1.1	NA	23.1.1	23.1.3
Policy	23.1.3	23.1.4	23.1.3	23.1.3	23.1.1	23.1.3	23.1.0	23.1.4	23.1.4	23.1.1	NA	23.1.1	23.1.3
Policy	23.1.2	23.1.4	23.1.2	23.1.2	23.1.1	23.1.2	23.1.0	23.1.4	23.1.4	23.1.1	NA	23.1.1	23.1.2
Policy	23.1.1	23.1.3	23.1.1	23.1.1	23.1.1	23.1.1	23.1.0	23.1.3	23.1.3	23.1.0	NA	23.1.0	23.1.1
Policy	23.1.0	23.1.3	23.1.0	23.1.0	23.1.0	23.1.0	23.1.0	23.1.3	23.1.3	23.1.0	NA	23.1.0	23.1.0
SCP	23.1.3	NA	NA	23.1.0	23.1.2	NA	23.1.2	NA	NA	23.1.2	23.1.2	NA	NA
SCP	23.1.2	NA	NA	23.1.0	23.1.1	NA	23.1.1	NA	NA	23.1.1	23.1.1	NA	NA
SCP	23.1.1	NA	NA	23.1.0	23.1.1	NA	23.1.1	NA	NA	23.1.1	23.1.1	NA	NA
SCP	23.1.0	NA	NA	23.1.0	23.1.0	NA	23.1.0	NA	NA	23.1.0	23.1.0	NA	NA
SEPP	23.1.4	NA	23.1.8	22.4.0	23.1.4	23.1.8	23.1.3	23.1.12	23.1.12	23.1.3	23.1.2	23.1.3	23.1.8
SEPP	23.1.3	NA	23.1.7	22.4.0	23.1.2	23.1.7	23.1.2	23.1.8	23.1.8	23.1.2	23.1.2	23.1.2	23.1.7
SEPP	23.1.2	NA	23.1.2	22.4.0	23.1.1	23.1.2	23.1.1	23.1.4	23.1.4	23.1.1	23.1.1	23.1.1	23.1.2
SEPP	23.1.1	NA	23.1.2	22.4.0	23.1.1	23.1.2	23.1.1	23.1.4	23.1.4	23.1.1	23.1.1	23.1.1	23.1.2
SEPP	23.1.0	NA	23.1.0	22.4.0	23.1.0	23.1.0	23.1.0	23.1.3	23.1.3	23.1.0	23.1.0	23.1.0	23.1.0

Table 3-3 (Cont.) Common Microservices Load Lineup for Network Functions

CNC NF	NF Version	Alternate Route Svc	App-Info	ASM Configuration	ATS Framework	Config-Server	Debug-tool	Egress Gateway	Ingress Gateway	Helm Test	Mediation	NRF-Client	Perf-Info
UDR	23.1.3	23.1.12	23.1.8	23.1.0	23.1.4	23.1.8	23.1.3	23.1.12	23.1.12	23.1.2	NA	23.1.3	23.1.8
UDR	23.1.2	23.1.9	23.1.7	23.1.0	23.1.2	23.1.7	23.1.2	23.1.9	23.1.9	23.1.2	NA	23.1.2	23.1.7
UDR	23.1.1	23.1.4	23.1.2	23.1.0	23.1.1	23.1.2	23.1.1	23.1.4	23.1.4	23.1.1	NA	23.1.1	23.1.2
UDR	23.1.0	23.1.3	23.1.0	23.1.0	23.1.0	23.1.0	23.1.0	23.1.3	23.1.3	23.1.0	NA	23.1.0	23.1.0

3.4 Security Certification Declaration

The following table lists the security tests and the corresponding dates of compliance for each network function:

Table 3-4 Security Certification Declaration

CNC NF	NF Version	Systems test on functional and security features	Regression testing on security configuration	Vulnerability testing	Fuzz testing on external interfaces
BSF	23.1.4	October 3, 2023	October 10, 2023	October 10, 2023	October 2, 2023
BSF	23.1.3	July19, 2023	July18, 2023	July18, 2023	July12, 2023
BSF	23.1.2	June 21, 2023	June 21, 2023	June 26, 2023	May 16, 2023
BSF	23.1.1	March 29, 2023	April 4, 2023	April 4, 2023	Feb 2, 2023
BSF	23.1.0	Feb 7, 2023	Feb 6, 2023	Feb 6, 2023	Feb 2, 2023
CNC Console	23.1.3	Oct 9, 2023	Oct 9, 2023	Oct 9, 2023	Feb 8, 2023
CNC Console	23.1.2	July 17, 2023	July 17, 2023	July 14, 2023	Feb 8, 2023
CNC Console	23.1.1	April 7, 2023	April 7, 2023	April 7, 2023	Feb 8, 2023
CNC Console	23.1.0	Feb 8, 2023	Feb 14, 2023	Feb 8, 2023	Feb 8, 2023
NEF	23.1.4	Oct 13, 2023	Feb 8, 2023	Oct 13, 2023	Feb 8, 2023
NEF	23.1.3	July 14, 2023	Feb 8, 2023	July 14, 2023	Feb 8, 2023
NEF	23.1.2	April 26, 2023	Feb 8, 2023	April 26, 2023	Feb 8, 2023
NEF	23.1.1	Feb 8, 2023	Feb 8, 2023	April 10, 2023	Feb 8, 2023
NEF	23.1.0	Feb 8, 2023	Feb 8, 2023	Feb 8, 2023	Feb 8, 2023
NRF	23.1.4	Oct 11, 2023	Oct 11, 2023	Oct 11, 2023	Oct 11, 2023
NRF	23.1.3	July 12, 2023	July 12, 2023	July 12, 2023	July 12, 2023
NRF	23.1.2	July 12, 2023	July 12, 2023	July 12, 2023	July 12, 2023
NRF	23.1.1	April 8, 2023	April 8, 2023	April 8, 2023	April 8, 2023
NRF	23.1.0	Feb 15, 2023	Feb 15, 2023	Feb 15, 2023	Feb 15, 2023
NSSF	23.1.2	July 14, 2023	July 14, 2023	July 14, 2023	July 14, 2023
NSSF	23.1.1	April 7, 2023	April 7, 2023	April 7, 2023	April 7, 2023
NSSF	23.1.0	Feb 16, 2023	Feb 16, 2023	Feb 16, 2023	Feb 16, 2023

Table 3-4 (Cont.) Security Certification Declaration

CNC NF	NF Version	Systems test on functional and security features	Regression testing on security configuration	Vulnerability testing	Fuzz testing on external interfaces
Policy	23.1.8	October 16, 2023	October 2, 2023	October 16, 2023	October 3, 2023
Policy	23.1.7	July 18, 2023	July 18, 2023	July 25, 2023	July 12, 2023
Policy	23.1.6	June 21, 2023	June 21, 2023	June 26, 2023	May 16, 2023
Policy	23.1.5	April 4, 2023	April 10, 2023	April 10, 2023	March 29, 2023
Policy	23.1.4	April 4, 2023	April 10, 2023	April 10, 2023	March 29, 2023
Policy	23.1.3	April 4, 2023	April 10, 2023	April 10, 2023	March 29, 2023
Policy	23.1.2	April 4, 2023	April 10, 2023	April 10, 2023	March 29, 2023
Policy	23.1.1	Feb 8, 2023	Feb 7, 2023	Feb 7, 2023	Feb 6, 2023
Policy	23.1.0	Feb 8, 2023	Feb 7, 2023	Feb 7, 2023	Feb 6, 2023
SCP	23.1.3	July 10, 2023	July 10, 2023	July 10, 2023	July 10, 2023
SCP	23.1.2	April 13, 2023	April 13, 2023	April 13, 2023	April 13, 2023
SCP	23.1.1	April 13, 2023	April 13, 2023	April 13, 2023	April 13, 2023
SCP	23.1.0	Feb 21, 2023	Feb 21, 2023	Feb 8, 2023	Feb 9, 2023
SEPP	23.1.4	Oct 12, 2023	Oct 12, 2023	Oct 12, 2023	Oct 12, 2023
SEPP	23.1.3	July 13, 2023	July 13, 2023	July 13, 2023	July 13, 2023
SEPP	23.1.2	June 12, 2023	June 12, 2023	June 9, 2023	June 9, 2023
SEPP	23.1.1	April 8, 2023	April 8, 2023	April 8, 2023	April 8, 2023
SEPP	23.1.0	Feb 15, 2023	Feb 15, 2023	Feb 15, 2023	Feb 15, 2023
UDR	23.1.3	NA (no new security features)	October 13, 2023	October 13, 2023	June 29, 2023
UDR	23.1.2	NA (no new security features)	June 29, 2023	June 29, 2023	June 29, 2023
UDR	23.1.1	NA (no new security features)	April 5, 2023	April 5, 2023	April 5, 2023
UDR	23.1.0	NA (no new security features)	Feb 17, 2023	Feb 17, 2023	Feb 15, 2023

3.5 Documentation Pack

All documents for Oracle Communications Cloud Native Core (CNC) 2.23.1 are available for download on SecureSites and MOS.

To learn how to access and download the documents from SecureSites, see Oracle users or Non-Oracle users.

To learn how to access and download the documentation pack from MOS, see Accessing NF Documents on MOS.

The NWDAF documentation is available on Oracle Help Center (OHC).

4
Resolved and Known Bugs

This chapter lists the resolved and known bugs for Oracle Communications Cloud Native Core release 2.23.1.

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.

4.1 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.

4.2 Resolved Bug List

The following Resolved Bugs tables list the bugs that are resolved in Oracle Communications Cloud Native Core Release 2.23.1.

4.2.1 BSF Resolved Bugs

BSF Release 23.1.4

There are no resolved bugs in this release. Resolved bugs from 23.1.x have been forward ported to release 23.1.4.

BSF Release 23.1.3

Table 4-1 BSF 23.1.3 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35671995	ENH 35671995 - diam-gw logging enhancement for IP-CAN_SESSION_NOT_AVAILABLE (5065)	When BSF Diameter Gateway was configured with logging level WARN, it did not print any logs while responding with DIAMETER error. For example, IP-CAN_SESSION_NOT_AVAILABLE (3GPP,5065).	3	23.1.2

Resolved bugs from 22.4.x have been forward ported to release 23.1.3.

BSF Release 23.1.2

Table 4-2 BSF 23.1.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35495540	BSF response with status code 404 for binding deletes	Due to race condition between Audit and Notify threads, an invalid queue reference was used by Notify thread which was not in synchronous with Audit Thread. This race condition was observed more, when the number of Audit and Notify threads were less than the number of tables to be audited.	3	22.3.1
35257657	BSF response with status code 400 for pcfbinding request	BSF was responding with 400 error code when PCF sent a POST request to create pcfbindings.	4	22.4.0

Note:

Resolved bugs from 22.4.x have been forward ported to release 23.1.2.

BSF Release 23.1.1

Table 4-3 BSF 23.1.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34900906	Update bsf alertRules template to include minor/ major/critical alerts	Updated BSF alertRules template to include minor/ major/critical alerts.	3	22.4.0
35257657	BSF response with status code 400 for pcfbinding request	PCF was sending a post request to create pcfbindings and BSF is responding with 400 error code.	4	22.4.0

Table 4-4 BSF ATS 23.1.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35040801	BSF response with status code 400 for pcfbinding request	PCF was sending a post request to create pcfbindings and BSF is responding with 400 error code.	2	22.4.0

BSF Release 23.1.0

There are no resolved bugs in this release.

4.2.2 CDCS Resolved Bugs

Table 4-5 CDCS 23.1.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35185267	CDCS does not support Cloud Native Configuration Console (CNC Console) ATS integration.	CDCS users are not able to download and run the CNC Console ATS suite.	4	• 23.1.0 • 22.4.0 • 22.3.0 • 22.2.0 • 22.1.0

Table 4-6 CDCS 23.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34915019	Not able to perform fresh OS install on CDCS BM host server	The CDCS host server doesn't perform a fresh OS installation of the host server during deployment.	2	22.3.1 22.4.0
34819844	NF Deletion job is not working	Unable to delete the NFs from 22.4.0 using the "Delete NF Release" pipeline. There is an error while performing the NF deletion and hence have to delete the NF manually.	3	22.4.0

4.2.3 CNC Console Resolved Bugs

CNC Console 23.1.3 Resolved Bugs

There are no resolved bugs in this release.

Table 4-7 CNC Console 23.1.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35545712	Validation-hook enhancement to support IPv6	Validation-hook has been enhanced to support IPv6.	4	23.1.0

Table 4-8 CNC Console 23.1.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35255733	Password displayed on CNCC Logs during update password	When the user updates the temporary CNCC credentials, the password is visible without masking the CNCC Logs files. This has been resolved by adding a loggingMasks filter in the cncc-iam.ingress-gateway.log.level.cncc section in the occncc_custom_values_<version>.yaml. This fix is available in CNC Console release 23.1.1 and 22.4.2.	2	22.4.1
35153278	CNCC cncc-mcore-igw pod taking continuously restarted after upgradation from 22.4.0 to 23.1.0 due to mismatch on requested issuer url (mCnccIams port)	The cncc-mcore-igw pod restarts repeatedly when CNC Console is upgraded from 22.4.0 to 23.1.0. This issue occurs due to a mismatch in the port. As a resolution, a note has been added in the Upgrade section of the CNC Console Installation, Upgrade, and Fault Recovery Guide to ensure that the mCnccIams port configuration is added only if port is other than 80.	3	23.1.0

Table 4-8 (Cont.) CNC Console 23.1.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35154799	The customer wants to Know the Trigger Conditions for Metrics	For cookie_routes (POLICY and BSF) Route_path is showing as unknown, and the queries and KPIs display empty results because of Route_path as unknown. As a fix for Policy and BSF, NFs ResourcePath is used in metric KPIs and expression is updated on the Grafana dashboard.	3	22.2.1
35106559	Console enhancement needed to access Promxy GUI Promxy API access works seamlessly via Console but for GUI access "/graph" needs to be manually appended.	"The user must add "/graph" manually to the Promxy GUI. As a resolution, an enhancement is made in release 23.1.1 to directly load the GUI from "/$OCCNE_CLUSTER/promxy/graph".	4	23.1.0

Table 4-9 CNC Console 23.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35082176	Replication issue after CNCC 22.3.1 fresh installation	Fresh intallation of CNC Console involves alter commands to modify schema. If applications perform alter commands, cn DBTier replication breaks. As a resolution, Console hook changes are made to create table schema before application startup.	2	22.3.1
34752687	Replication goes down in 4 Site GR setup during CNCC fresh installation	Fresh installation of Console involves alter commands to modify schema. If applications perform alter commands, DbTier replication breaks. As a resolution Console hook changes are made to create table schema before application startup.	2	22.3.0

Table 4-9 (Cont.) CNC Console 23.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34906369	Prod CNCC: BB CNCC Upgrade to 22.2.1 caused Replication Channel down alert	Fresh installation of CNC Console involves alter commands to modify schema. If applications perform alter commands, cnDBTier replication breaks. As a resolution Console hook changes are made to create table schema before application startup.	2	22.2.1
35047812	CNCC MIB does not comply estandar RFC2578	CNCC MIB files have some errors that make the CNCC MIB fail in the compilation process. As a resolution, corrections have been made in MIB files and have been validated using the MIB validator.	3	22.4.0
34753994	alert CnccCoreAccessTokenFailure received with user unknown	The prometheus alert, CnccCoreAccessTokenFailure, which indicates a failed login attempt, does not carry enough information to identify the user or origin of attempt. It says username is unknown.	4	1.9.2
34780743	Traffic feed option not visible in CNCC after a fresh login	The traffic feed option in CNC Console is not visible after a fresh login. After that if you switch to any other namespace from the select instance dropdown, and then switch it back to the SCP namespace, then the traffic feed is visible.	4	22.4.0

Note:

Resolved bugs from 22.3.x and 22.4.x have been forward ported to release 23.1.0.

4.2.4 Policy Resolved Bugs

Policy 23.1.8 Release

There are no resolved bugs in this release. Resolved bugs from 23.1.7 have been forward ported to release 23.1.8.

Table 4-10 Policy 23.1.7 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35671200	500 errors on sm create on multiple sites after applying config	After applying the golden configuration, error 500 appeared on SM create on multiple sites.	2	23.1.6, 23.2.0
35661401	cnPCF_FT: Stale session - SM sessions are not audited after enabling the Audit from PCF GUI	SM Service audit was not scheduled even after enabling it from PCF GUI.	3	22.3.1
35563740	UpdateNotify 503 retry	After SMF failover, SMPCF was sending UpdateNotify to the secondary SMF, but received response 503 (pkt 606/608).	3	23.1.5

Note:

Resolved bugs from 23.1.6 have been forward ported to release 23.1.7.

Table 4-11 Policy 23.1.6 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35529351	SupportedFeatures as null, sent in the update response to SMF	The update response to SMF was sent with "SupportedFeatures" as null.	2	22.3.0
35248922	Traffic getting rejected with Error Timeout processing for event: Latency: 4173ms\nDiameter:Sent	The traffic was rejected with error timeout processing for the event: Latency: 4173ms\nDiameter:Sent.	2	22.4.5
35456086	Post PCF upgrade from 22.4.5 to 23.1.4 audit pods are high in using resources	On PCF upgrade from 22.4.5 to 23.1.4, it was observed that the audit pods were using more CPU resources.	2	23.1.4

Table 4-11 (Cont.) Policy 23.1.6 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35235857	On PCF upgrade to 23.1.0, the audit service with high load	Due to race condition between Audit and Notify threads, an invalid queue reference was used by Notify thread which was not in synchronous with Audit Thread. This race condition was observed more, when the number of Audit and Notify threads were less than the number of tables to be audited.	2	23.1.0
35519200	5GC GETS call failures	5GC was getting call failures on Rx call flows without Media Component Description (MCD).	3	22.4.0
35525606	Post site isolation, site2 traffic moved to site1 we observed td-ms entry missing in site1 and targeted traffic at site1 was not achived to 15KTPS.	Post the site isolation, when site2 traffic was moved to site1, it was observed that the td-ms entry was missing in site1 and the targeted traffic of 15K TPS at site1 was not achieved.	4	22.4.5

Note:

Resolved bugs from 23.1.5 have been forward ported to release 23.1.6.

Table 4-12 Policy 23.1.5 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35411508	PCF responding with incorrect session QoS after receiving SMF Updates with RAT type change	Upon receiving the SMF update, SM was overriding the PRE QoS information with the QoS in the SMF Update instead of sending the PRE provided session QoS information.	2	22.4.5

Note:

Resolved bugs from 23.1.4 have been forward ported to release 23.1.5.

Table 4-13 Policy 23.1.4 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35360635	Policy Export Functionality failure with certain blockly - "Set session revalidation time to earliest of"	Policy Export Functionality failed with "Set session revalidation time to earliest of" blockly.	3	23.1.3
35365705	Mismatched waitforCHF value	SM Pod was sending out a value different from waitforCHF than determined by the PRE pod.	3	23.1.3
35378747	Default # of Max Rx Session set to 2 in 23.1.x	In SM-Rx, only two Rx sessions were being allowed to be created by default.	3	23.1.3
35378622	403 LATE OVERLAPPING REQUEST for SM Request	When two different SMs were coming for different DNN we are seeing 403 Error Late Overlapping request.	4	23.1.1

Note:

Resolved bugs from 23.1.3 have been forward ported to release 23.1.4.

Table 4-14 Policy 23.1.3 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35266983	PCF sends N1N2Subscription every time when PCF attempts to send URSP rule	PCF sent N1N2Subscription each time PCF attempted to send the URSP rule.	2	22.4.1
35308123	Unable to Create multiple tables using Table Slicing	The user was unable to create multiple tables using table slicing.	2	23.1.2
35310800	BULK Import EXPORT not working for extra large files >1 MB	Bulk Import and export was not working for extra-large files greater than 1 MB.	3	22.2.6
35329572	SM Service sending extra Null attributes towards SMF	SM Service was sending extra null attributes towards SMF.	3	23.1.1

Note:

Resolved bugs from 23.1.2 have been forward ported to release 23.1.3.

Table 4-15 Policy 23.1.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34889642	SPAD_POLICY_PERF During Performance runs for Policy Performance pod (perf-info)restarting multiple times and error observed "Failed to establish a new connection"	During performance runs for Policy performance pod (Perf-info) and restarted multiple times. The error observed is "Failed to establish a new connection".	2	22.4.0
35170483	RAA with 5002 Error Response does not trigger N7 session cleanup	RAA with 5002 error response did not trigger N7 session cleanup.	2	22.3.3
35210135	IGW timeout observed in PCF as a result of crash at SMF	Ingress Gateway timeout was observed in PCF as a result of crash at Session Management Function (SMF).	2	22.3.3
35216078	Unable to install cnPCRF 23.1.0	cnPCRF 23.1.0 installation failed with timeout error.	2	23.1.0
35219220	IGW time out observed because of High CPU in PRE	Ingress Gateway timeout was observed because of high CPU utilization in PRE.	2	22.3.3
35270008	PCF Stale SM Sessions seen w/o PDS on 23.1.x release	In Policy 23.1.x release, stale SM Sessions were observed without PDS DB *table entries with Source Type 0 - (SSV Values default).*	2	23.1.1
34993721	HTTP TRACE Method Enabled	There was an issue with the HTTP TRACE method configuration.	3	22.2.1
35240414	Warn Log in Object Expression exception scenario is filling the logs	The default logging level for WARN was changed to DEBUG as WARN log in an object expression block was filling the logs.	3	22.4.4
35240443	PRE shall wait for config server communication for atleast 3 seconds for performance	PRE waited for at least 3 seconds while trying to fetch the data from config server and the requestTimeout was changed to 3000.	3	22.4.4
35246656	PCF does not set the fqdn/ port correctly in notficiationUrl in Binding Service	PCF was setting the notification URL to what is set in BINDING_APIROOT instead of pcfApiRoot.	3	22.4.0
35207903	Session state variable not working as expected	Session state variable was not working as per the expectation.	4	22.4.1
35245854	Error "calledStationId is not found in either Request or in Session" on pcrf-core pods while running 7.5k tps traffic each site on a 4 site GR setup	Error "calledStationId is not found in either Request or in Session" was shown on pcrf-core pods while running 7.5k TPS traffic per site on a 4 site georedundancy setup.	4	22.4.5
35262859	PRE not able to read data from config server and results in frequent Error Logs	PRE was not able to read data from config server, which resulted in frequent error logs.	4	22.3.2

Table 4-15 (Cont.) Policy 23.1.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35272033	mySqlDbCompressionEnabled and mySqlDbCompressionScheme parameters are not present in Policy custom.yaml file	*mySqlDbCompressionEnabled* and *mySqlDbCompressionScheme* parameters were not present in Policy custom-values.yaml file.	4	22.4.5
35225677	All SOAP POST requests from OneNDS failing with HTTP 500	All SOAP POST requests from OneNDS ware failing with HTTP 500.	4	22.4.1

Note:

Resolved bugs from 23.1.1 have been forward ported to release 23.1.2.

Table 4-16 Policy 23.1.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35071477	No SLR seen towards OCS, TIME_WAIT occurring between diam-conn and gateway pod	Diameter-Gateway and Diameter-Connector do not respond after a couple of hours (No response for TCP SYN Message from Simulator) and are not able to connect with any peers.	2	22.3.2
35149654	PCF-ATS 23.1.0 : Issue in PRE evaluation for Rx Multiple Media Components	When setting the numericMax Ul/Dl and numericGbr Dl/Ul values, the calculation of 0.05 over 4.0 Mbps is applied, resulting in 200 Kbps for both component media (AUDIO and VIDEO), while expectation is to keep the values received in the Rx request on the SM session over every media component/sub media component.	3	23.1.0

Table 4-16 (Cont.) Policy 23.1.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35152551	pcrf-core pod in crashloopback off after 22.4.2 voice policy upgrade	Port 9000 in PCRF Core is mapped to METRIC_PROMETHEUS_PORT and instead needs to be mapped to *MONITORING_PORT* in order to make the metric port configurable.	4	22.4.2
35161311	PCF No New N28 message during race condition of smf CREATE & DELETE requests	When CHF Connector pod restarts during upgrade or pod boot, dataSourceRouteCtxtMap gets reset. After this, when PDS sends a PUT or Delete message to CHF Connector, a NPE is encountered with the the data source route context being searched by fqdn.	4	22.3.3
35162261	PCF sending empty header packet to BSF after 22.3.3 Upgrade	When BSF registration fails, it does not save location header in the database. Whenever there is a Delete request, there is no validation whether BSF registration was successful which results in setting 3gpp-sbi-target-apiroot as [[null://null]].	4	22.3.3
35163279	SPAD_POLICY LDAP response metrics are not updated correctly in case failure response from LDAP	In case of 400 failure response, LDAP Gateway reports both 4xx and 5xx failure metrics.	4	22.4.0

Table 4-16 (Cont.) Policy 23.1.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35164870	Alerts on "new state : CONGESTED" and could see OutOfMemoryError on newly added diam-gateway pods	Diameter Gateway attempts multiple trials to reconnect to the peer even when reconnectLimit is set to 0 in the peer configuration during one discovery cycle.	4	22.4.5

Note:

Resolved bugs from 23.1.0 have been forward ported to release 23.1.1.

Table 4-17 Policy ATS 23.1.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35143848	ATS 23.1.0 Feature Local_Profile failed due to path issue in the feature file	Local_Profile feature failed due to non-parameterized path usage in the feature file.	3	23.1.0

Table 4-18 Policy 23.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34964990	UE Policy Message Size shall support bigger range	The range for the 'N1 Message Maximum Size' and 'UE Policy Section Maximum Size' from 0 to 9000 Bytes is not supported. This range should be fixed, or else operators will not be able to put bigger values for the range and messages will get unnecessarily fragmented.	3	22.4.0
35119770	PCF AM UI error: Query user is enabled on GUI but internal configuration shows otherwise	PCF AM UI error: Query user is enabled on GUI but internal configuration shows otherwise.	3	23.1.0

Table 4-19 Policy ATS 23.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34644934	PCRF core rejecting the traffic with diameter authorization rejected with 5003	PCRF core rejects the traffic with diameter authorization which is rejected with 5003.	3	1.15.0

4.2.5 cnDBTier Resolved Bugs

Table 4-20 cnDBTier 23.1.3 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35139386	During CNDB upgrade from 22.4.1 to 23.1.0, multiple restarts can be observed in ndbmysql pods	When General Query Log feature was enabled in 23.1.0 during the upgrade from 22.4.1 to 23.1.0, the feature on replication SQL pod did not work, which led to continuous restart of container.	1	23.1.0
35410102	DR failure due to error: remotesitedatanodecount.properties does not exists	When the backup transfer failed and was retried, the `/var/occnedb/dbbackup/remotesitedatanodecount.properties` file was removed.	2	23.1.1
35724053	SLF/cnDBTier 22.4.3 db_tier_backup{status="FAILED"} prometheus alert	The *Backup failed* alert was not cleared from the backup info table while performing backup.	2	22.4.3
35643518	Channel switchover leading to replication break on multi channel setup	Switchover failed to resume in case of REST API timeout due to some network delay.	2	23.2.1
35740004	DBTier Installation Guide: SiteId in the yaml file need to be set as 1, 2, 3, 4	It was required to set SiteId in the yaml file as 1, 2, 3, and 4 corresponding to each site as an unique set identifier.	2	23.1.0
35130162	Unable to deploy a 3 or 4 site MultiChannel setup with 6 channels	Unable to install cnDBTier with more than 14 replication SQL pods in 3 or 4 site MultiChannel setup with 6 channels.	2	22.3.2
35789704	During rollback of CNDB from 23.2.1 to 23.1.1, replication breaks and db-backup-manager pod is stuck in crashloopbackoff	Two Hop rollback with different versions is not supported by MySQL/cnDBTier.	2	23.1.1

Table 4-20 (Cont.) cnDBTier 23.1.3 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35711068	22.4.3 Vertical Scaling of ndbappmysqld pods has nothing for its PVC	There was an ask to include vertical scaling procedure for PVC and modify vertical scaling procedure for the ndbappmysqld.	3	22.4.3
35395995	Alert BINLOG_STORAGE_FULL since installing 22.3.2	BINLOG_STORAGE_FULL alert is raised if apiReplicaCount is 0 and repl sql pvc is set to 0.	3	22.3.1
35364251	DBTier 22.4.1 alert's expression issues	The alert descriptions lacked clarity in specifying when the alert would automatically be cleared.	3	22.4.1
34997129	Clarification on DBTier Automated Backup behavior	The time zone of the db-backup-manager-svc and db-backup-executor-svc had to be changed to UTC as cronitor package did not support the deployment time zone.	3	22.4.0
35590372	cnDBTier 23.2.0 MIBs and alertrules don't match	cnDBTier 23.2.0 MIBs and alert rules did not match.	3	23.2.0
35734862	Helm chart takes wrong startNodeId for ndbmysqld from custom values.yaml	The environment variable “STARTING_SQL_NODEID" was incorrectly set to “70” instead of “56” in the ndbmysqld statefulset for the init-sidecar container.	3	23.1.2
35504362	Replication svc pvc is not getting recreated on pod deletion, if in state of termination	The replication svc pvc was not recreated when the pod was deleted and in the termination state.	3	23.1.1
35798774	CNDBTier 23.3.0 Installation is failing via CDCS	cnDBTier installation failed while using CDCS.	3	23.3.0
35829082	REPLICATION_SKIP_ERRORS_LOW alarm is firing for cnDBTier	REPLICATION_SKIP_ERRORS_LOW alarm was raised for cnDBTier when replication halted due to skip error count less than equal to 5. Also, replication broke while performing worker node upgrade.	3	23.2.1
35372063	Skip error feature for CNDBTier not working when using site id as 5 and 6 for a 2 site GR setup	Skip Error feature was not working when using site id as 5 and 6 for a two-site georeplication setup. Instead, there was a need to add an equation to assign server id.	3	23.1.0
35432969	Listing the changes made in the CNDBTIER MOP 22.4.2 for engineering approval	There was a need to verify if the changes listed in the MOP are documented in the GA docs.	4	22.4.2

Table 4-21 cnDBTier 23.1.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35139386	During CNDB upgrade from 22.4.1 to 23.1.0, multiple restarts can be observed in ndbmysql pods	Rotation of general query log on replication SQL pod was not working leading to continuous restarts of ndbmysqld pods.	1	23.1.0
35097185	During CNDB upgrade from 22.1.1 to 22.2.5, multiple restarts can be observed in CNDB pods.	Backup manager service pods restarted multiple times during an upgrade. This is a normal behavior observed when the backup manager service encounters an error. Therefore, cnDBTier documents are updated with notes regarding self restarts of backup manager service in case of errors.	1	22.2.5
35194625	Data loss observed along with 'Binary log cache data overflowed to disk 577 time(s). Consider increasing --binlog-cache-size' error in sql logs	The Liveness probe used the root password to query the database mysqld pods. When the root password was changed, the Liveness probe failed and the pods restarted. The dbtpasswd script was also restarting the pods simultaneously which caused the replication pods associated with a channel to be rebooted at the same time.	1	23.1.0
35274059	CNDB restart of mysqld pod during the upgrade	Rotation of general query log on replication SQL pod was not working leading to continuous restarts of ndbmysqld pods.	2	23.1.1
35260142	Replication not working post upgrade using vCNEEgress feature	Egress network annotations were getting added to the services instead of the deployment pods. As a result, the IP rules were not getting added to the worker nodes.	2	23.1.0
35193206	PROD PCF ACTIVE SESSIONS WENT DOWN to ZERO ON SOUTH LAKE due to NDB cluster restart	Replication failure was observed at customer's site. To fix the issue, configuration options are included in the values.yaml file to configure GCP monitor and LCP parameters.	2	22.3.3
35192902	PROD PCF ACTIVE SESSIONS WENT DOWN to ZERO ON SOUTH LAKE, all nDB MTD pods having one of it's containers restart	Replication failure was observed at customer's site. To fix the issue, configuration options are included in the values.yaml file to configure GCP monitor and LCP parameters.	2	22.3.2

Table 4-21 (Cont.) cnDBTier 23.1.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35350673	DBTier replication failure seen during NFVI testing	Replication failure was observed at customer's site. To fix the issue, configuration options are included in the values.yaml file to configure GCP monitor and LCP parameters.	2	22.4.1
34618463	Horizontal Scaling of ndbmtd pods	The horizontal scaling of ndbmtd pods procedure in the cnDBTier user guide required updates regarding the sequence to be followed while creating node groups.	2	22.3.0
35523597	cnDBTier MoP Updates:steps for ndbappmysql pod scaling with service accout and autoscaling disabled	cnDBTier user guide was missing steps to horizontally scale ndbappmysqld when autoscaling is disabled.	3	23.1.1
35494876	SQL pods stuck in crashloop on cndb 23.2.0 after restore with backup taken on 22.4.1	cnDBTier backup and restore were not supported for different cnDBTier versions.	3	23.2.0
35335531	GR state is retained as "COMPLETED" when DR is re-triggered	The gr_state was retained as "COMPLETED" when the user retriggered the fault recovery on a cnDBTier setup.	3	23.1.1
35249301	Automatic restart of pod not happening when the standby ndbmysqld had a crashed binlog thread	Replication pods were not restarted automatically when the standby ndbmysqld pod had a crashed binlog thread.	3	22.4.1
35202648	DR Guide Refinement Request, re: 4-Site Geo-Replication	Fault recovery procedures in the cnDBTier Fault Recovery Guide required certain refinements and additional information.	3	22.4.1
35249321	Automatically purge some binlog on startup if it is full to avoid pod going in crashloopbackoff state	The binlog files were not automatically purged on startup. This caused the binlog to overflow leading to replication failures.	3	22.4.1
35116989	DBTier MIB does not comply with standard RFC2578	cnDBTier MIB did not comply with the RFC2578 standard.	3	22.4.1
35259935	Enhance DR logging to display the exact point and cause of failure	Customer requested for alerts when there is a failure in file transfer from one pod to other pod, or from one site to another site.	3	23.1.0
35524871	DBTier password Change Procedure Failed	The dbtpasswd script required specific updates to run in the customer environment.	3	23.1.1

Table 4-22 cnDBTier 23.1.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35125409	Replication breaks and same error observed in ndbmysql pod in two scenarios - MTA feature is not working	Georeplication broke on MTA enabled cnDBTier setups. As a result, MTA feature had to be disabled.	2	23.1.0
35217746	NRF 23.1 cnDBTier Rollback Failure	Rollback failed while running the `hooks.sh --post-rollback` script from Bastion Host.	2	23.1.0
35130162	Unable to deploy a 3 or 4 site MultiChannel setup with 6 channels.	Installation of cnDBTier with more than 14 replication SQL pods was not successful.	2	22.3.2
35207810	cnDBTier upgrade from 22.2.1 to 22.4.1 broke replication between sites	occneuser and occnerepluser are hard coded in the cnDBTier helm chart. Therefore, if a username is created different from the occneuser or occnerepluser, it causes the replication to break during an upgrade.	2	22.4.1
35118514	Scaling procedure for ndbmtd pods does not work as expected	Fault recovery procedure must support database restore when the data node replica counts are different than that in the remote cnDBTier cluster.	3	22.3.4
35182608	cnDBTier alert rules fail to load in 22.4.x due to incorrect alert indentation in cnDBTier_Alertrules.yaml file	cnDBTier alert rules failed to load due to incorrect indentation of BINLOG_INJECTOR_STOPPED and HEARTBEAT_FAILED alerts in the `cnDBTier_Alertrules.yaml` file.	3	22.4.2
35113031	GRR fails while unable to delete DB from NF nwdaf	Automated georeplication fault recovery procedure got stuck while trying to drop databases with "-" (dash) in their names.	3	22.1.1

Table 4-23 cnDBTier 23.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34674761	mysqld process crashed when the Application which is connected to the NDB cluster is getting upgraded.	On querying the database, the ndbmysqld pod restarted and the replication channel was stuck with the "the incident LOST_EVENTS occurred on the master. Message: mysqld startup" error.	2	22.3.0
35084355	Removing the old backups stored in the replication service in case transfer of backup failed	While performing a fault recovery, the old backups stored in the replication service pod PVC had to be deleted if transferring the backup failed.	3	23.1.0
35084371	Format SLAVE_REPLICATION_DELAY_HIGH description	Local Replication service was not updating the remote backup transfer status in case of failure.	3	23.1.0
35056129	Proper formatting should be there in summary of SLAVE_REPLICATION_DELAY_HIGH SNMP alert	The SLAVE_REPLICATION_DELAY_HIGH alert description required a formatting fix.	3	22.4.0
34826194	Modify ndb(mt)d to ignore SIGCHLD	The ndbmtd MySQL cluster update process required a modification to ignore SIGCHLD.	3	22.2.0
34654470	Copying ALTER safety check false positives	On querying the database, the ndbmysqld pod restarted and the replication channel was stuck with the "Duplicate column name 'lastAuditedTime'' error. The details of the default database and the query are as follows: Default Database: 'occnp_binding'. Query: 'ALTER TABLE occnp_binding.contextbinding ADD COLUMN lastAuditedTime.."	3	22.3.2

Note:

Resolved bugs from 22.2.5, 22.3.4 and 22.4.1 have been forward ported to release 23.1.x.

4.2.6 CNE Resolved Bugs

Table 4-24 CNE 23.1.4 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36139899	alertmanager secrets configuration is wrong after update	After an upgrade from 23.1.3 to 23.2.5, the SNMP notifier service was migrated from `occne-snmp-notifier` to `occne-alertmanager-snmp-notifier`, however the alertmanager configuration didn't reflect this change.	3	23.2.5

Table 4-25 CNE 23.1.3 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35089494	Opensearch Index Management Operations are not working	Entire Index management lifecycle failed due to the following reasons: • OpenSearch Index management operations failed. • Indexes did not transition from hot to warm state. • Force merge and delete did not work for any indexes.	2	23.1.1
35182156	LBVMs unable to communicate with backend services	Load Balancer Virtual Machines (LBVM) were unable to communicate with the backend services as the k8s Security Group (SG) overrided the k8s_node_secgroup SG. To overcome this issue, both the k8s and k8s_node_secgroup SGs that are applied to the worker nodes are combined.	2	22.4.1
35168065	High CPU usage on CNE 22.4.1 nodes	Individual master nodes showed high CPU usage while other master nodes had very low usage.	2	22.4.1

Table 4-25 (Cont.) CNE 23.1.3 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34978552	After Upgrade to 22.3 VMware LBs are left with dysfunctional ifcfg file	After CNE upgrade on VMware cluster, most of the STANDBY LBs and several ACTIVE LBs were left with a dysfunctional /etc/sysconfig/networking-scripts/ifcfg-ens192 file.	2	22.4.0

Table 4-26 CNE 23.1.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35471163	removeBmWorkerNode.py does not completely remove a BM node	While running the script to automatically remove Kubernetes worker node in a Bare Metal cluster, the script was not performing the following actions: 1. Logging to an external file (removeBmWkrNodeCapture-${DATE}.log) was not called. 2. While removing the OSD, the script left a phantom negative ID related to the removed node. This ID was not completely removed.	3	• 23.1.1 • 23.2.0
35307224	Complete switchover didn't happen after replication LBVM failure	The boot.log file in the /var/log directory of the LBVM was filled by logs generated by a python script and was not getting rotated. This resulted in the LBVM disk space getting full which subsequently led to a LBVM failure.	3	• 23.1.1 • 23.2.0
35339676	sync_bastions script design has permissions issues that will break synchronization in multiple scenarios	Bastion registry is currently run as root. This leads to problems with rsync cron job in some cases where a root created registry image needs to be deleted after switchover.	3	• 23.1.1 • 23.1.0 • 22.4.2 • 22.4.1

Table 4-26 (Cont.) CNE 23.1.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35334779	sync_bastions script creates duplicated keys within known_hosts file	Customer has reported an issue wherein the sync_bastions script appears to be creating duplicate SSH key entries within the known_hosts file on the bastions. As this file grows in size, SSH logins begin to slow down noticeably.	3	• 23.1.1 • 23.1.0 • 22.4.1

Table 4-27 CNE 23.1.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35145909	Deploy fails due to Not enough IPs are available for the desired node count	When deploying more than 64 nodes, the deployment failed during Kubernetes preinstall check stating "Not enough IPs are available for the desired node count".	2	• 23.1.0 • 22.4.1
35061535	OpenSearch GUI doesn't show complete SCP log	During the log forwarding process in FluentBit, in some cases, it was observed that FluentBit stalled to ingest data in OpenSearch. During the issue investigation, it was found that the source of the issue was the OpenSearch index creation process. OpenSearch index creation process blocked (indexblock) ingestion API calls when the cluster observed high disk usage or high compute usage, leading to HTTP 403 errors.	2	23.1.0

Table 4-28 CNE 23.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34830696	addPeerPool.py (Adding External Network) doing test_cluster fails	The pipeline call to configure the new LBVMs was also running the cluster test which resulted the script to fail. The cluster test was not to be run at that point in the script and needed to be corrected.	2	22.1.0 22.2.1 22.2.2 22.3.0 22.3.1 22.4.0
34690860	Pipeline script failed for ILO reboot: OCCNE 22.3.0	When the pipeline script is run from the Bastion Host 2, the task to reboot or restart the ILO servers failed as there was no route to host.	2	22.1.3 22.2.2 22.3.1
34712083	ServiceIP port not attached properly in the LBVM for production site	Adding a service with more than two ports and adding a namespace with a number that is equal to or less than the number of ports in the service, changed the namespace name and created a duplicate entry in the haproxy.cfg file.	2	22.1.0 22.2.1 22.2.2 22.3.0 22.3.1 22.4.0
34644768	OCCNE K8S_UPGRADE FAILING	CNE upgrade failed due to timeout on pod draining operations which had to be ignored.	3	22.1.0 22.2.0 22.3.0 22.4.0
34644811	/var/log/messages file size zero in LBVM	A postrotate script is set in the provision log_config task for running the logrotate program. This postrotate script must get rsyslog to reload the /var/log/ messages file and other file handles after rotation, but it was not working.	3	22.1.0 22.2.0 22.3.0 22.4.0
34644351	Lb-Controller Database not being updated correctly	Not all LBVM pairs got updated with the new worker node external IP in the haproxy.cfg file. As a result, the server was not included in the HA functionality of haproxy.	3	22.3.0 22.4.0

Table 4-28 (Cont.) CNE 23.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34854251	Issues Identified in the CNE Installer script	The CNE installer reads provisioning data from the cluster.tfvars file. This file contains IP ranges as metallb IP pool parameters. The installer uses python scripts to translate those IP ranges into flat IP lists. However, the «flattenRange» function in the «scripts/genMbAutoTfvars.py» script had a bug that lead to incorrect list generation.	3	22.1.0 22.2.1 22.2.2 22.3.0 22.3.1 22.4.0

Note:

Resolved bugs from 22.3.3 and 22.4.1 have been forward ported to release 23.1.0.

4.2.7 NEF Resolved Bugs

Table 4-29 NEF 23.1.4 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35804622	All NEF services are not working in model-D deployment.	In Model-D, the header format of all npcf-policyauthorization services was invalid and was rejected at NRF.	1	23.3.0
35763438	TI subscription with External Group ID is giving error as "Routing Rule not found"	TI subscriptions which includes an External Group ID were receiving the following error: Routing Rule not found	3	23.2.0

NEF 23.1.3 Resolved Bugs

There are no resolved bugs in this release.

Table 4-30 NEF 23.1.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35202851	During In-service upgrade, the failure rate is 1.3% and there is complete loss in traffic for few seconds.	During the in-service upgrade, the failure rate is 1.3% and there is a complete loss in traffic for a few seconds.	2	23.1.0
35199184	After upgrade 2 out of 5 fiveGCoreEGW pods are taking very less traffic than the other pods	After the upgrade, two fiveGCoreEGW pods are processing less traffic than the other pods.	3	23.1.0
35199207	After upgrade, only 2 out of 5 ME pods are handling notification traffic	After the upgrade, only two ME pods are processing the notification traffic.	3	23.1.0
35262686	Delete Security Method API is not working	The delete security method API is not working.	3	23.1.0
35199227	Traffic is not distributed equally between the pods in the microservices	Traffic is not getting distributed equally between the pods in the microservices 5GCoreEGW, External EGW, NEF-ME Stats (ReqRate AMF-ME otifications,ResponseRate ME Notifications), and 5GCAgent Stats (ResponseRate ME Subscription).	4	23.1.0

Table 4-31 NEF 23.1.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35142862	In in-service upgrade of NEF from 22.4.1 to 23.1.0, aef-apirouter pods are not coming up	The aef-apirouter pods were not installed while performing in-service upgrade of NEF from 22.4.1 to 23.1.0.	2	22.4.1
35228285	capif-afmgr pod is restarted if we give expire time more than 11 days in capif yaml file	If expire time was set to more than 11 days in the oc-capif-custom-values.yaml file, the capif-afmgr pod restarted.	3	23.1.0

Table 4-32 NEF 23.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34967716	Due to missing information in header from NEF in DELETE /nudm-ee/v1..SCP is unable to route.	Due to the missing 3gpp-sbi-producer-id header information, the DELETE subscription flow failed in SCP for model D.	2	22.4.0

Table 4-32 (Cont.) NEF 23.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35062697	NEF - PCF Media-Type parameter is needed to support successful AFSessionwithQOS initial setup	AFSessionwithQOS requires mediaType in Npcf_Authorization flow towards OC PCF. NEF includes configurable mediaType based on the QosReference attribute received in 3gpp-as-session-with-qos AF request.	3	22.4.1
35020419	ME Events allowing to subscribe MSISDN with More than 15 digits	As per 3gpp, MSISDN should have a maximum of 15 digits, but NEF is allowing more than 16 digits. NEF needs to reject request received with MSISDN having more than 15 digits.	3	22.4.0
34916378	NEF ATS GUI Documentation tab do not display details of testcases	Documentation tab on GUI does not display the list of testcases and its details.	3	22.4.0
34803406	NEF Pre-provisioned ApiInvoker update	OAuth token is associated with the ApiInvoker expiry. There is no option to configure if the invoker expired. It requires operators to delete and recreate to make any required change.	4	22.2.2

4.2.8 NRF Resolved Bugs

NRF 23.1.4 Resolved Bugs

There are no resolved bugs in this release.

Table 4-33 NRF 23.1.3 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
35515800	NRF 23.1.1 closing active TCP connections after 2 mins	In NRF 23.1.1 release, active TCP connections closed after 2 mins.	2	23.1.1
35751680	NRF 22.4.2 notified NF status for AMFs NOT within the same AMF set (amfSetId+amfRegionId)	As per 29.510, NRF must send a notification when both amdSetId and amfRegionId conditions are met. NRF is only checking for matching amfSetId, whereas NRF must check for both amfRegionId and amfSetId.	2	22.4.2

Table 4-33 (Cont.) NRF 23.1.3 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
35782188	NfProfile is being saved with NRF with port: 0 if port is absent in ipEndPoints	NfProfile saved with NRF with port: 0, if port is not present in ipEndPoints.	3	22.2.0

Table 4-34 NRF 23.1.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
35314965	NRF not sending mateScpInfoList in profile retrieval 23.1.0	NRF was not sending `mateScpInfoList` in profile retrieval when `mateScpInfoList` was empty in customInfo. **Note:** This bug has been backported from 23.2.0.	2	23.1.0
35286843	Error code 503 is observed across all NRF operations during 12K TPS performance run on each site	Error code 503 was observed across all NRF operations during 12K TPS performance run on each site. **Note**: This bug has been backported from 23.2.0.	2	23.1.0
35291189	OCNRF 23.1.0 Upgrade from 22.4.0 fails with "unknown anchor 'imagePullPolicy' referenced"	Upgrade from 22.4.0 to 23.1.0 failed with "unknown anchor 'imagePullPolicy' referenced". **Note**: This bug has been backported from 23.2.0.	2	23.1.0
35417911	InterPlmnFQDN is coming in NFServiceList attribute during Discovery Response	InterPlmnFQDN was coming in NFServiceList attribute during Discovery Response. **Note**: This bug has been backported from 23.2.0.	3	23.1.1
35427205	NRF 23.1.0: non-regression on accessToken not authorized in roaming out scenario	Access Token Authorization was getting skipped even when NF type was present in the Access Token Request Body.	3	23.1.0

Table 4-34 (Cont.) NRF 23.1.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
35566636	NRF 23.1.1 responding with 200 OK for Heartbeat service operation when Load is changed	NRF 23.1.1 was responding with 200 OK for Heartbeat service operation when NF load was changed. NRF now sends 204 No content as HTTP Response code whenever load is changed in heartbeat service operation.	3	23.1.1
35600211	Heartbeat: Load attribute in nfServiceList need to be considered as Heartbeat like with NFStatus and Load at NFprofile and NFservice	Load attribute in nfServiceList needs to be considered as Heartbeat with NFStatus and load at NFprofile and NFservice.	3	23.1.1
35416406	NRF 23.1.1 is including interPlmnFqdn parameter in nfProfile for Notification Events	`InterPlmnFqdn` attribute in nfProfile is present for NFStatusNotify request generated by NRF.	3	23.1.1
35117440	Network Policies Errors - After installing the policies, the notification messages towards the remote site SCP is failing	Network Policies were updated to send notification messages toward the remote site SCP successfully. Network Policies are provided over the bug and fixed in the 23.1.2 release.	3	22.4.0
35600621	NFStatusNotify service operation NFProfile returning nfSetIdList in uppercase	`NFStatusNotify` service operation in NFProfile was returning `nfSetIdList` in uppercase even when NF was registered with lower case value.	3	23.1.1
35600657	OCNRF not decoding exploded array elements in the query properly	NRF was not decoding exploded array elements in the query properly, and it was decoding only the first value of such attributes.	3	23.1.1
35417836	Network Policy is not allowing connections from different namespace	Network Policy was not allowing connections from different namespace to NRF Ingress Gateway. **Note**: This bug has been backported from 23.2.0.	3	23.1.1

Table 4-34 (Cont.) NRF 23.1.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
35417814	Discovery Cache is not refreshing records for Custom NFs	Discovery Cache is not refreshing records for Custom NFs. **Note**: This bug has been backported from 23.2.0.	3	23.1.1

Table 4-35 NRF 23.1.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
35271694	Roaming Updates: During NFStatusSubscribe message relaxation of plmnId attribute presence in request for vNRF case	When the Roaming Feature is enabled, during NFStatusSubscribe request handling, if the *reqPlmnList* attribute is present in the request body and the attribute value matches with NRF PLMN, the NRF is considered as vNRF, and *plmnId* is not present in the request. In this case, NRF processes the request message locally and treats the message for Intra-PLMN routing instead of rejecting the request due to absense of *plmnId* attribute in the request.	3	22.4.1
35271698	Roaming Updates: During NFAccessToken message relaxation of targetPlmn attribute presence for vNRF case	When the Roaming Feature is enabled, during AccessTokenReq handling, if *requesterPlmn* attribute is present in the request body and the attribute value matches with NRF PLMN, the NRF is considered as vNRF, and *targetPlmn* is not present in the request. In this case, NRF processes the request message locally and treats the message for Intra-PLMN routing instead of rejecting the request due to non-presence of *targetPlmn* attribute in the request.	3	22.4.1

Table 4-35 (Cont.) NRF 23.1.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
35255363	NRF - Incorrect command parameter "nrfInstanceId" under Section 6.3 Deleting the MySQL Details	The command to delete the instanceid was incorrect in the "Deleting the MySQL Details" section of *Oracle Communications Cloud Native Core, Network Repository Function Installation, Upgrade, and Fault Recovery Guide*.	4	23.1.0

Table 4-36 NRF 23.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
35057941	Locations in location Set must have length between 5 and 100	Location name in location set configuration has character limit of 5 to 100. The requirement is to configure locations even less than 5 characters. Character length check is removed for location while configuration.	2	22.4.0
35073240	Users from mysql.user were removed after DR in site3	After Database back up is applied, User and Grants has to be created manually. As they would not be part of backup file. This is documented.	2	22.2.2
34568765	UDR not getting added to "slfDiscoveredCandidate List" for NRF when registered with more than one "nfService"	If UDR NF profile contains more than one NFservice then slfDiscoveredCandidate List is not getting populated for Dynamic SLF selection. The requirement is that the slfDiscoveredCandidate List must populated as per Dynamic SLF selection feature when NFservice list contains more than one NFService.	3	22.2.2
35103955	NF Discovery forwarding returning empty response	When NF Discovery forwarding happens to another NRF and second NRF not returning suspended NF profiles with empty list feature enabled.	3	22.4.1

Table 4-36 (Cont.) NRF 23.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
34737232	Error Getting Metrics in app-info and performance pods	It is observed that errors are shown in kibana logs related to app-info and performance services.	3	22.3.0
34942732	Default values assigned to threadpool & applicationthreadpoolconfig to be corrected	Default values assigned to threadpool & applicationthreadpoolconfig must be corrected.	3	22.4.0
35103968	Remove checks for requester-features in the case of preferred-tai support	Remove checks for requester-features in the case of preferred-tai support. Currently, preferred-tai support is dependent upon requester-features attribute presence and its value. Checks for requester-features attribute while processing preferred-tai is removed	3	22.4.1
34924288	The topicName from custom-values.yaml should be corrected	Data director would consume the traffic for aggregation only if thedata received on the topic named 'NRF' and hence the request is to make the changes onto default yaml to have topic name as 'NRF'. "NRF" is set as default value for topicName in custom-values.yaml	4	22.4.0
34863029	NRF alerts OcnrfTotalNFsRegisteredApproachingMinorThreshold documention BUG	OcnrfTotalNFsRegisteredApproachingMinorThreshold alert will cause continues "firing" once the threshold is approached which contradict with the information in the documentations.	4	22.1.4

Note:

Resolved bugs from 22.4.1 has been forward ported to release 23.1.0.

4.2.9 NSSF Resolved Bugs

NSSF 23.1.2 Resolved Bugs

There are no resolved bugs in this release.

Table 4-37 NSSF 23.1.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35149048	NSSF ATS 23.1.0: unable to configure pipeline	To trigger a build, it is required to change some parameters in the pipeline and save. However, the user was not able to save the changed configuration. After selecting the save option, the user was getting HTTP 403 error.	2	23.1.0
35114407	10K TPS has glitches when ASM/mTLS is enabled on dbtier	NSSF must support 10K TPS with ASM. However, it was failing to do so.	2	23.1.0
35209131	Error 422 occurred for procedure "avail-patch" during traffic run with 2.5K TPS NSSF	Error 422 occurred for procedure "avail-patch" during a traffic run with 2.5K TPS on NSSF.	3	23.1.0
35191414	PV parameters are not present in ATS values.yaml	PV parameters such as `PVEnabled` and `PVClaimName` were not present in ocats-nssf-custom-values.yaml. However, these parameters are present in the 22.4.3 ocats-nssf-custom-values.yaml file. These parameters must be present in ocats-nssf-custom-values.yaml as well.	3	23.1.0
35191006	Subscription-Patch-Unsubscription is not working in 3 site GR Setup	In 3 site GR setup, while sending a POST Nssai Subscription request, it was throwing an error.	3	23.1.0
35188822	In amf_tai_snssai_map table, amf_set_id is incorrect format while using amf_id present in amf_resolution table.	amf_set_id was in an incorrect format in amf_tai_snssai_map table. It was observed while using amf_id present in the amf_set and amf_resolution table.	3	23.1.0
35174619	Issue with Availabilty put in 3-site GR setup	While running ns-availability-put traffic on different sites, the user was getting duplicate entry issue.	3	23.1.0

Table 4-37 (Cont.) NSSF 23.1.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35149397	NSSF ATS 23.1.0: GR_NSAvailability_PUT is getting failed	The GR_NSAvailability_PUT feature was getting failed in regression pipeline. In previous version of NSSF 22.4.2, this feature was one of the new features that were passed. The reason behind this was "ocnssf-db-creds" secret name, which was hardcoded in the regression pipeline. Even after passing the parameter "o" as appuser-secret, it was not picking up the correct value.	3	23.1.0
35138414	For Same AMF-ID, SNSSAI, MCC, MNC and TAC NsAvailability PUT is not working for other sites	For the same AMF-ID, SNSSAI, MCC, MNC, and TAC NsAvailability, PUT was not working for other sites.	3	23.1.0
35138363	NSAvailabality Delete is not working in GR Setup	While running performance test in a GR Setup that run NsAvailability PUT, NsAvailabilityDelete and again NsAvailability PUT together, it was showing an error for duplicate entry in the NsAvailabilityData table.	3	23.1.0
35178788	Success rate dropped and internal server error occurred in Ingress pod while running traffic with 2.5K TPS on Debug Build	The success rate dropped and the internal server error occurred in the Ingress pod while running traffic with 2.5K TPS.	3	23.1.0
35095820	IN NSI Profile, NRF Access Token URI is mandatory parameter in CNCC UI	NRF Access Token URI should be mandatory in CNCC GUI, but it was showing as optional.	3	22.4.2
35052539	NSSF is not sending the expected data for log level	CNCC GUI was not showing any default log level for all NSSF services.	3	22.4.2

Table 4-37 (Cont.) NSSF 23.1.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35266672	NSSF- Documentation error causing helm test failure	While following NSSF Installation, Upgrade, and Fault Recovery Guide's section: 2.2.1.4, 'Creating Service Account, Role, and RoleBinding', the manually created API resources passed the names in the ocnssf-23.1.0.0.0.custom-values.yaml file. However, the Helm test failed with error messages.	3	23.1.0

Table 4-38 NSSF 23.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35062375	while changing the NF Status (AMF) Suspended State to Registered State, NSSF is sending 404 Not found for notification response	While changing the NF Status (AMF) from Suspended State to Registered State, NSSF is sending 404 not found for notification response.	2	22.4.2
35041907	While adding the Amf-set in CNCC UI, OCNSSF send invalid parameter in subscription request towards NRF	While adding the Amf-set in CNCC UI, NSSF sends an invalid parameter in the subscription request towards NRF.	2	22.4.2
35014512	Indirect Communication not working for NSSF, available default custom yaml missing many SCProuting params	Indirect communication is not working for NSSF. The available default custom yaml file is missing many SCProuting parameters.	2	22.4.0
35006379	amf_tai_snssai_map table has contained duplicate entry because of nsavailability scenarios are not working	amf_tai_snssai_map table has duplicate entries because of which nsavailability scenarios are not working.	2	22.4.1
34990487	Internal Server error occurred in Ingress pod while running traffic with 2.5K/1K tps with perfgo and timeout happening for NSSF Procedures	Internal server error occurs in Ingress pod while running traffic with 2.5K/1K TPS with perfgo, resulting in timeout of NSSF procedures.	2	22.4.1

Table 4-38 (Cont.) NSSF 23.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34976534	ocnssf-nsavailability pod crashed beacuse of OutOfMemoryError: : Java heap space	ocnssf-nsavailability pod crashes beacuse of OutOfMemoryError: : Java heap space error.	2	22.4.1
34939923	ocnssf-nssubscription service pod is not coming up while doing upgradation from Version 22.3.1 to 22.4.1	ocnssf-nssubscription service pod is not coming up while upgrading from version 22.3.1 to 22.4.1.	2	22.4.1
35050609	NSSF EANAN feature: if the sNSSAI is deleted, NSSF does not sent a notify	NSSF EANAN feature: if the sNSSAI is deleted, NSSF does not send a notification.	3	22.4.0
35004536	ocnssf-nsavailability CPU Usages reaches too high (100%)	ocnssf-nsavailability CPU usage reaches high levels (100%).	3	22.4.1
34898985	NSSF ATS 22.4.1 | ATS Version in ATS GUI is wrong	NSSF ATS 22.4.1 | ATS Version in ATS GUI is wrong.	3	22.4.1
34868500	UE Config Update: ConfiguredNssai must be present	UE Config Update: ConfiguredNssai must be present, but it is not present.	3	22.3.0
34797626	NSSF 22.3 Auto-Population of Configuration Based on NsAvailability	The user is not able to run "/nnssf-nssaiavailability/v1/nssai-availability/07c4ca5a-68aa-4d7c-960c-c7a523 2378c1". The user is getting the following error: {"type":"INTERNAL_SERVER_ERROR","title":"DB_READ_WRITE_ERROR","status":500,"detail":"Could not execute delete AuthorizedNssaiAvailabilityInfo viaamfid","instance":"null","cause":"INTERNAL_SERVER_ERROR"} (Logs attached)	3	22.3.0
34784403	NSSF 22.3.0 : Nokia AMF profile not supported in NSSF	While registering the Nokia AMF profile with tacRangeList with NRF, the NSSF selection request is not successfully returning the candidateAmfList.	3	22.3.0

Table 4-38 (Cont.) NSSF 23.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35035092	Document issues in NSSF_Installation_and_Upgrade_Guide 22.4.2	The user noticed some errors with some commands mentioned in the installation guide. Also, the default values of some parameters in the guide are different from custom-values.yaml file.	3	22.4.2
35038558	NSSF: Few errors in the REST Specification Guide	A few of the NSSF REST APIs are not working as expected in the documentation.	4	22.4.2

4.2.10 SCP Resolved Bugs

Table 4-39 SCP 23.1.3 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35506935	Validation for metric ocscp_worker_outstanding_requests was failing intermittently	Validation for the ocscp_worker_outstanding_requests metric was failing intermittently. A fix was added to the ATS feature file to avoid these intermittent failures.	3	23.1.2
35468748	SCP changes snssais format in the delegated discovery request from SCP to NRF	SCP was modifying some of array attributes when sending delegated discovery request to NRF.	3	23.1.1
35583704	Host header to be removed before sending request to Mediation	SCP was sending host header in message requests toward Mediation resulting in istio sidecar failure to route the messages.	3	23.2.0

Table 4-40 SCP 23.1.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35328103	SCP upgrade failure for load manager microservice	SCP upgrade from 22.4.2 to 23.1.1 failed at the preupgrade hook stage because SCP-Load-Manager microservice version was not recognizable.	2	23.1.1
35317027	ApiFullversion format in NF Profile nfServices should support x.x.x.x version number format	The ApiFullversion format in NF Profile nfServices must support the x.x.x.x format.	2	23.1.0

Table 4-40 (Cont.) SCP 23.1.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35298113	OutlierDetectionProducer_AUSF.feature getting failed on full regression run	The OutlierDetectionProducer_AUSF.feature failed during regression run due to metrics mismatch.	2	23.1.1
35215530	Inter SCP routing failing when Inter PLMN fqdn format is received in 3gpp-sbi-apiroot-target	The Inter SCP routing failed when the Inter PLMN fqdn format was received in the 3gpp-sbi-apiroot-target header.	3	23.1.0
35306715	SCP ATS Regression NRF_Subscription Scenarios failed	Successful reregistration resulted in the additional thread for heartbeats leading to duplicate heartbeats of SCP toward NRF.	3	22.4.2

Table 4-41 SCP 23.1.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35225956	Egress host preference NF type resolution not working for HTTPS	The Egress host preference for NF type resolution is not working for HTTPS.	2	23.1.0
35251392	S1 test case failing under the SCP_Egress_Host_Preference_SMF_P0_P1 feature feature	In the Egress_Host_Preference feature test cases, the stub queue cleanup step was missing that caused intermittent failures while running the test cases.	2	23.1.0
35113063	Prometheus restart observed due to high number of samples	Enables or disables of dimensions such as "ocscp_nf_instance_id" and "ocscp_service_instance_id" as configurable.	2	22.2.2
35114091	SCP taking NF FQDN as null from NFProfile in Model-D https call when IpEndpoints and FQDN is null at service level	While making a Model-D call, SCP is taking NF FQDN as null from NFProfile IpEndpoints and FQDN are null at service level.	3	22.4.0
35210347	SCP sends RST_STREAM to NSSF requests	When AMF is sending nnssf-nssaiavailability request to NSSF though SCP (Model C) and SCP receives a deregistration notification about this AMF instance from NRF after it forwarded the nnssf-nssaiavailability request to NSSF, SCP sends RST_STREAM to NSSF without waiting for response from NSSF.	3	22.4.0

Table 4-41 (Cont.) SCP 23.1.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35254166	SCP ATS New Features OutlierDetectionInterSCP Failure	OutlierDetectionInterSCP failed due to incorrect validation in the feature file.	3	22.4.1
35292662	Notification processing failure resulting in resource mapping deletion in some exception cases	Unable to restore deleted resourceMappings for rel15 rule processing whenever there is an exception during SCP Notification processing.	3	22.2.2
35180678	Egress_congestion_based_on_producer_load_and_message_priority_UDM Scenario-8 failed	ATS is enhanced to check whether notified profile is updated in DB at a later time or not rather than checking the last 30 seconds.	3	23.1.0
35188493	SCP_Observability_And_Inter_Microservice_Resilience feature is failing	Pod scaling was taking more time than expected resulting in intermittent failures.	3	23.1.0
35292697	SCP ATS Outlier Detection scenario failing with code 403 for put operations	The issue identified in the feature file was not passing the system options values correctly.	3	22.4.2
35267919	SCPFailureHandling_EnhancedServerHeaderV2_p0 feature is failing in new-feature run	Server header received as null on scaling down pods on the ASM setup. The fixed feature file to be agnostic to platform.	3	23.1.0
35267896	Scenarios of Alert_SCPIngressTrafficRateExceededConfiguredLimit.feature failing	Scenario was failing as it was conflicting with other scenario where topology source for the NF was made local.	3	23.1.0
35286494	Enhanced_NF_Status_Processing_SUSPENDED_SMF.feature failed during full Regression Run	Scenario was failing due to NF profiles deregistration conflict with other scenarios.	3	23.1.0
35269258	RateLimitingRelease16_AUSF.feature failed due to metrics issue in parallel execution	The RateLimitingRelease16_AUSF scenario was failing due to nfInstanceId conflict with other scenario.	3	23.1.0
35251882	EgressRateLimiting_UDM_Cases.feature failed during parallel execution	The EgressRateLimiting_UDM_Cases scenario was failing due to nfInstanceId conflict with other scenario.	3	23.1.0
35185170	"HTTP ERROR 403" issue while trying to configure pipeline in ATS Gui	The "HTTP ERROR 403" issue was received while trying to configure pipeline in the ATS GUI.	3	23.1.0

Table 4-42 SCP 23.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35028366	GlobalEgressRateLimiting.feature:5 fails due to Values are not close	Validated the ocscp_metric_egress_rate_limiting_not_applied_req_total metric in rate limiting scenarios.	2	22.4.1
34751247	30K MPS traffic towards DD : 1.4% Traffic feed is not copied to DD & marked as "Not Attempted"	Few messages were discarded due to the increase of scp-worker CPU resulting in message not being copied to Data Director (DD).	2	22.3.0
35081909	SCP sending 503 due to Circuit breaking condition not clearing	Total transaction timeout on SCP resulted in Circuit Breaking count with stale values. This caused some traffic failures on SCP.	2	22.2.1
34537811	Restarting the mediation pod after applying rules does not recover the mediation pod	Configmap reference in environment variable was resulting in pod crash when number of rules are high. Removed unecessary reference from environmrent variable to fix the issue.	3	22.3.0
34579260	Console SCP GUI - SCP Routing Options json file has duplicate id	In Console SCP GUI, SCP Routing Options json file has duplicate ID.	3	22.3.0
34581772	CPU utilization of some worker pods reached 7 when traffic was running at 230K TPS	CPU utilization of some worker pods reached 7 when traffic was running at 230K TPS due to intermittent timeout errors. SCP's timer and threads are optimized to fix the issue.	3	22.3.0
34043568	2-2.5K 429's are observed in the performance run where ASM is enabled	Some error were observed during performance run. SCP's timer and threads are optimized to fix the issue.	3	22.1.1
34348059	Audit and subscription pods are in 0/1 state when trying to register 10 NRF Profiles (With TLS and Without ASM)-DB descrepencies are seen	Issue observed during virtual service creation for NRF profiles. Exception handling improved to fix the issue.	3	22.1.1
34355882	Observed that ocsp_response_code 503 is returned from mediation to worker during the performance run	Intermittent errors were observed from mediation during performance run. Mediation libraries uplifted and timers optimized to fix the issue.	3	22.2.0
34452952	Mediation is not printing Ingress request params to make debugging easy	Request headers and Request body are printed now as part of Mediation logs when the request message landed on Mediation for debugging purpose.	3	22.2.1

Table 4-42 (Cont.) SCP 23.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34452955	Incorrect Mediation Logs	Rules Applied Statistics were incorrect resulting in the issue. Fixed Statistics in Mediation.	3	22.2.1
34463825	SCP is sending incorrect notification URI in SM policy create request	SCP was incorrectly updating the callback URI in notifications when reverse proxy flag was enabled.	3	22.2.0
34780164	Ingress Rate Limiting doesn't appear to work with User Agent NFType for Consumer NF	Ingress rate limiting based on only NFType in User agent is not supported as there is no definitive way to derive unique nfInstanceId. Software is updated to handle the use case.	3	22.3.1
34813639	Worker pods CPU utilization alerts triggering unexpectedly	SCP CPU calculation logic is enhanced to capture average number of intervals configured to fix the issue.	3	22.2.2
34830689	Questions regarding TCP keepAlive settings not supported	TCP keepAlive was not enabled for upstream connections. The same is now enabled in 23.1.0 release and document is updated as well.	3	22.3.1
34838348	SCP Model-D performance degradation observed.	Intermittent errors during performance run was resulting in high scp-worker memory. Software is optimized to avoid such errors.	3	22.4.0
34842720	ATS REL16 New Feature test case got failed	scp-worker was generating exception while sending response for NRF Notification at Log Level DEBUG resulting in ATS failure.	3	22.4.0
34856989	SCP Local Rate Limit does early rejections of messages compared to configured rate	Rate Limit logic enhanced to reduce early requests throtlling.	3	22.4.0
34864454	OD functionality for SEPP is not working because of dependency of SEPP OD audit on SCP config	The Outlier Detection functionality for SEPP is not working because of dependency of SEPP OD audit on SCP config.	3	22.4.0
34874277	CNCC SCP GUI - Help links are not working	CN Configuration Console SCP GUI Help links are not working.	3	22.3.0
34920034	New line and Tabs (\n & \t) appearing in 5g-sbi-message at Kafka	New line and Tabs (\n & \t) appearing in 5g-sbi-message at Kafka.	3	22.4.0

Table 4-42 (Cont.) SCP 23.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34942445	SCP returns 500 internal error in case of LCI parameter is missing while configuring LCI in SCP features	SCP returns 500 internal error in case Load Control Information (LCI) parameter is missing while configuring LCI in SCP features.	3	22.4.0
34963539	PCF not visible in NF Rule Profile in SCP after registration in NRF	Api version such as 1.1.0.0 was not handled correctly and thus NF profiles was rejected by SCP.	3	22.3.0
34967750	SCP does not match routing rule when 3gpp-sbi-target-apiroot contains capital letters	SCP does not match routing rule when 3gpp-sbi-target-apiroot contains capital letters.	3	22.3.0
34973838	"ocscp_metric_nf_set_unhealthy" is not updated when all producer NFs in a NF Set are marked outlier and Alert is not generated	"ocscp_metric_nf_set_unhealthy" is not updated when all producer NFs in an NF Set are marked outlier and alert is not generated.	3	22.4.0
34990807	Need to update rest specification guide table 2-27 for attribute max-payload-size	Oracle Communications Cloud Native Core, Service Communication Proxy REST Specification Guide is updated with the max-payload-size parameter.	3	22.2.0
35001544	Ingress_Rate_Limiting_enhancement_for_nfInstanceId_to_support_UserAgentHeader failing	Alerts were taking longer than expected to clear on the setup. Maximum wait time in ATS is increased to accomodate the delay.	3	22.4.1
35007432	Audit and Subscription pods issue when SCP deployed with more than one NRF	Audit and Subscription pods issue occurred when SCP was deployed with more than one NRF and when service level FQDN was not provided in NRF Profiles.	3	22.3.3
35012313	Incorrect timestamp format in SCP Microservices logs	Inconsistent Timestamp format was observed in some of SCP Microservices logs.	3	22.3.3
35015609	After Alert_SCPIngressTrafficRateExceededConfiguredLimit-Scenario 3 Failure and others need retry	ATS is enhanced to wait for longer duration to account for delay in Alert trigerring and clearing.	3	22.3.2
35030722	SMF-UDM Model D: Generated 3gpp-sbi-target-apiroot includes trailing slash / if path pseudo-header not in UDM response	Removed Trailing slash from SCP added 3gpp-sbi-target-apiroot header in case of Dest-Reselection for modelC and modelD response back to consumer NF.	3	22.3.0

Table 4-42 (Cont.) SCP 23.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35031092	SCP-DD connection failure resulting in back to back scp-worker restarts	scp-worker restart was observed during performance testing with Data Director. SCP timeouts values are optimized to fix the issue.	3	22.4.1
35042977	File Name Reference Inconsistency within CSAR Package	Inconsistent naming convention was used across different files in csar package.	3	22.3.4
35066632	SCP is not sending its own LCI while sending the response from interSCP to unknown peer	SCP is not sending its own LCI while sending the response from interSCP to unknown peer.	3	23.1.0
35094376	Ingress_Rate_Limiting_enhancement_for_nfInstanceId_to_support_UserAgentHeader failing	Intermittent ATS failure was observed due to delay in fetching metrics. Testcase is optimized to handle this delay.	3	22.4.2
34535976	During 48 hours of traffic, one of the worker pods' memory consumption exceeded major threshold	Intermittent errors during performance run was resulting in high scp-worker memory. Software is optimized to avoid errors.	4	22.3.0
34477800	Helm warning, apiVersion policy/v1beta1 PodDisruptionBudget is deprecated in v1.21	PodDisruptionBudget Api version is updated as per latest Kubernetes support to fix the issue.	4	22.2.1
34588080	Correct title of CNCC screen "Ingress Rate Limiter Consumer Info"	Title of the screen is modified to Consumer Info configuration from Ingress Rate Limiter Consumer Info.	4	22.3.0
34713119	Validation of NFInstance Id is not happening during inter SCP connectivity when federation is enabled	Error Log is added in case incorrect NFInstance ID is configured for remote SCP cache cluster.	4	22.4.0
34977360	Additional "scp_fqdn" parameter is coming for "ocscp_metric_nf_unhealthy_total"	Additional scp_fqdn parameter is added for the ocscp_metric_nf_unhealthy_total metric.	4	22.4.0
34949599	"Peerscpfqdn" parameter is showing incorrect value for Alert(SCP Unhealthy Peer SCP Detected)	The Peerscpfqdn parameter value is showing error for the SCPUnhealthyPeerSCPDetected alert.	4	22.4.0
34838586	reRouteOnResponseCodeList is not mentioned at NF Service level in SCP REST GUIDE	Oracle Communications Cloud Native Core, Service Communication Proxy REST Specification Guide is updated with the reRouteOnResponseCodeList field is indicated at NF Service level.	4	22.3.0

> **Note:**
>
> Resolved bugs from 22.4.2 have been forward ported to release 23.1.0.

4.2.11 SEPP Resolved Bugs

Table 4-43 SEPP 23.1.4 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35208390	SEPP-Upgrade: cn32f and pn32f pods restart observed during cndb rollback	cn32f and pn32f pods were restarting during the cnDBTier rollback to 23.1.x release.	3	23.1.0

> **Note:**
>
> Resolved bugs from 22.4.x and 23.1.x have been forward ported to Release 23.1.4.

Table 4-44 SEPP 23.1.3 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35478340	Gets 400 and 500 error codes from Egress Gateway, when requests are routed to multiple SEPPs.	When the traffic was sent from consumer SEPP to one Producer Remote SEPP, performance was consistent. But while sending the traffic to more than one Producer Remote SEPPs, the Gateway displayed the error and the user could not run the traffic beyond 70 TPS.	2	23.1.2

Table 4-44 (Cont.) SEPP 23.1.3 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35603146	SEPP Rollback fails when security feature configuration is done on upgraded setup.	After performing an upgrade from 23.1.x or 22.4.x release to 23.2.x release, perform the security feature configuration through REST API or CNC Console. Configuration will be successful and tables will have the latest data. But, while performing a rollback from 23.2.x. to 23.1.x or 23.4.x release, the rollback fails with foreign key reference.	3	23.1.2

Note:

Resolved bugs from 22.4.x and 23.1.x have been forward ported to Release 23.1.3.

Table 4-45 SEPP 23.1.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35375298	SEPP reporting Error 500 "No Matching Route."	This error condition was causing the route deletion at the gateway. Hence, was not able to download the correct route for routing. Now, optimized the creation of routes at gateway.	2	22.3.1
35470937	After SEPP upgrade, 500 Internal Server error is observed for the Discovery messages.	The 3gpp-sbi-target-apiroot header was removed when the message was going out of C-SEPP.	2	23.1.1

Table 4-45 (Cont.) SEPP 23.1.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35337221	SEPP ATS installation failed on Tanzu Cluster	SEPP ATS installation failed on Tanzu Cluster. `helm install ocats ocats-sepp-23.1.2.tgz -f ocats_ocsepp_values_23.1.2_ys-sepp_v1.yaml -n ys-sepp` The following error occured: "unable to build kubernetes objects from release manifest: [unable to recognize “”: no matches for kind “ServiceEntry” in version “networking.istio.io/v1alpha3”, unable to recognize “”: no matches for kind “VirtualService” in version “networking.istio.io/v1alpha3”]"	2	23.1.1
35488504	isEnabled=False functionality is not working as expected	Without changing isEnabled to True, handshake was created and peer was created in common configuration table. Also, the user was unable to delete the remoteSepp when isEnabled was set to False.	3	23.1.1
35379697	SEPP upgrade from 22.3.0 to 23.1.0 fails and SEPP installation fails when Debug tools and Mediation are enabled.	The SEPP upgrade from 22.3.0 to 23.1.0 failed when the Debug tools and mediation were enabled. The 23.1.0 installation failed when Debug tools and Mediation were enabled together.	3	23.1.0

Table 4-45 (Cont.) SEPP 23.1.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35407842	Partner SEPP rejecting n32 handshake due to Oracle SEPP including advisorCount parameter in JSON payload	Partner SEPP rejected n32 handshake due to the Oracle SEPP including `advisorCount` parameter in JSON payload.	3	23.1.1
35211643	SEPP Upgrade and Install: SEPP pods deployment edit required for OSO integration after SEPP fresh install and upgrade	After following the steps for SEPP integration with OSO during SEPP installation and upgrade, SEPP deployment edit was required. It caused SEPP pods to restart.This is service impacted in case of upgrade. Here is the change: before: `oracle.com/cnc: \"true\` after: `oracle.com/cnc: "true".` Extra characters were not replaced which caused the user to edit the service and remove the characters.	3	23.1.1

Table 4-46 SEPP ATS 23.1.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35297819	Unable to access ATS GUI in ASM	After the successful deployment of ATS in ASM, the user was not able to access the UI for bddclient.	2	23.1.1

Table 4-47 SEPP 23.1.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35176943	cn32f pods restarted due to OOMKilled (exit code 137) and call failed observed with 504 & 503 Error during SEPP performance run	When running the SEPP traffic at 62K MPS, Egress Gateways are displaying the 503 and 504 error codes randomly after every two minutes. This is due to the new timer added in Ingress Gateway and Egress gateway; `nettyIdleTimeout`. Default value of this timer is set to 2 minutes: nettyIdleTimeout: 120000 Set the default value of this timer in plmn-egress-gateway and n32-egress-gateway to 120000000. This will not reset the jetty connection after every two minutes and will not generate 503 and 504 error messages.	2	23.1.0
35208657	DBTier_Rollback: SEPP Pods restart leading to missing SEPP tables post CNDB rollback from 23.1.0 to 22.4.0 causing complete traffic failure	Few tables are removed from SEPP Database during the cnDBTier rollback from 23.1.0 to 22.4.0, resulting in complete traffic failure. SEPP pods cn32f and pn32f restarted during the cnDBTier rollback. This occurs when config-mgr-svc is restarted after the cnDBTier rollback. This is due to an issue in alter table command that is used to update the Dbengine to NDBcluster (for CNE setup). As a fix, the alter table command is removed from config-mgr-svc code.	2	23.1.0
35211643	SEPP Upgrade and Install: SEPP pods deployment edit required for OSO integration after SEPP fresh installation and upgrade	After performing the steps for SEPP integration with OSO during SEPP installation and upgrade, SEPP deployment must be edited. As a result of the edit, SEPP pods restart. This impacts the upgrade. As a fix, the following changes are integrated: oracle.com/cnc: \"true\ is changed to oracle.com/cnc: "true". Extra characters are not getting replaced. As a result, the user has to edit the service the remove them.	3	22.4.2
35168315	SEPP-Rollback: PLMN Ingress and Egress and config manager pods not up and complete traffic loss after sepp rollback from 23.1.0 to 22.4.2	PLMN Ingress Gateway, Egress Gateway, and config manager pods are not up and running, and complete traffic loss is observed after SEPP rollback from 23.1.0 to 22.4.2. This is because a service account is created in 23.1.0. When a rollback is performed on an earlier release, service account is looked upon, which does not exist in earlier release. Hence, the rollback fails.	3	23.1.0

Table 4-47 (Cont.) SEPP 23.1.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35215773	SEPP-SOR: SOR feature PUT request example needs to be updated	There are discrepancies in User, Installation, and REST API guides related to the SOR feature. Hence, the documents are updated.	3	23.1.0
35126068	Re-init field is updated to N32F_ESTABLISHED_STATE at the producer side	The details about the re-init field and the corresponding allowed state are added in the SEPP REST API Guide.	4	22.4.0

Table 4-48 SEPP 23.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35047400	SEPP MIB does not comply estandar RFC2578	Some errors are observed that make the SEPP MIB fail in the compilation process and it has to be changed manually.	3	22.4.0
35021336	Cache cleanup issue at Cn32f leading to display of incorrect error code.	CN32F service internal cache was not cleaned up and refreshed properly. Due to this, old data and error code were not getting displayed.	3	22.4.0
35014084	406 Error codeand Call failure observed on"supi" uri service's with default header configuration for Security Counter Measure_Cat2	Call failure observerved on "supi" uri services with default header configuration for Security Counter Measure Cat-2 feature and 406 Error code is being observed. Another issue observed is when 14 digit IMSI is configured, it was pass, but for IMSI(15 digit) it gets failed.	3	22.4.0
34988847	SEPP 22.3.1 deployment fails due to config-mgr-svc taking too long to initialize	Due to the latency issues, in some of the networks config-mgr-svc takes long time to initialize. Due to this, liveliness and readiness fails and service gets times out. Fixed the issue by increasing the timeout value.	3	22.4.0
34953499	HostedSEPP adding two via header in request and response flow	Hosted SEPP adding two via header in request and response flow - one from cn32f-svc and other from pn32f-svc as both the services are in the single flow. Removed the via header added by cn32f-svc while running in Roaming hub/ Hosted SEPP mode. via header will be added only by pn32f-svc.	3	22.4.0

Table 4-48 (Cont.) SEPP 23.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34939411	RemoteSEPPSet Creation Error via CNCC after P-RSS enabled	When the SEPP is deployed in Hosted SEPP mode and P-RSS feature is enabled, Remote Sepp Set creation starts getting failed at CNC console. It can be configured through REST API. This is due to code merge issues observed between hosted SEPP and sSecurity Countermeasure feature. one feature overwritten the file changes of other. Fixed the code for the same.	3	22.4.0
34527183	SEPP adding both Server and via header if next hop is down	SEPP Installation documentation is updated. In gateway helm parameter section, added the details of nfInstanceID and definition of server header.	3	22.2.0
34627763	n32f_jetty, cn32f_jetty, pn32f_server_latency and cn32f_server_latency metrics are not being pegged	Following metrics are not being logged: • ocsepp_pn32f_jetty_request_stat_metrics • ocsepp_cn32f_jetty_request_stat_metrics • ocsepp_pn32f_server_latency • ocsepp_cn32f_server_latency Updated the code to display the above metrics.	3	22.4.0
34987139	HostedSEPP: "Direction" dimension needs be removed from user guide	Direction dimension in some of the metrics in SEPP User Guide was incorrect and not as per the code. Updated the SEPP User Guide and made it in sync with the code.	4	22.4.0
34974178	nfInstanceId is displayed twice in alert SEPPN32fServiceApiValidationFailureAlert	nfInstanceId is displayed twice in alert, SEPPN32fServiceApiValidationFailureAlert. due to the incorrect code handling. Fixed the code and now nfInstanceId is displayed only once.	4	22.4.0
34969699	Dimensions to be corrected for metric ocsepp_security_service_api_failure_total	Document Issue: peer_domain dimension is not present in the ocsepp_security_service_api_failure_total metric output but it is documented in user guide. The SEPP user guide has been updated.	4	22.4.0
34969602	Response code and error message needs correction when user tries to delete AL associated to RSS	If the user tries to delete an allowed list associated with a Remote SEPP Set, incorrect error code and message is displayed. The error message was as follows: "Please update allowed name in remote partner set before deleting". The error message has been updated to "Please update allowed list name in remote partner set before deleting".	4	22.4.0

Table 4-48 (Cont.) SEPP 23.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34969002	HostedSEPP: SEPP feature list api returns 404	An extra API is added in REST API guide and not being used in the code. The REST API sepp-configuration/v1/sepp-feature-list is deleted. SEPP REST API document also updated.	4	22.4.0
34954936	Proper error should be thrown if invalid body is passed to enable SCM	To enable CAT -2 Network ID Validation feature, if an ivalid body configuration is passed, the following error displayed. JSON parse error: Unexpected character ('}' (code 125)): expected a value; nested exception is com.fasterxml.jackson.databind.JsonMappingException: Unexpected character ('}' (code 125)): expected a value. The code has been fixed to display the appropriate error.	4	22.4.0
34946120	Table 3-4 and 3-5 needs to be updated for RequestRejectStatusCodeName	Document issue: SEPP installation guide Table Configuration parameters section has incorrect default value for RequestRejectStatusCodeName parameter. Updated the document and made it as per the with the code.	4	22.4.0
34934348	Error message has typo in response payload when incorrect 3gpp-sbi-target-apiroot is provided	When incorrect 3gpp-sbi-target-apiroot is provided and request is sent, then the response received has typo in it. The response was as follows: "cause":"3GPP Target SBI AbiRoot wrong syntax". Instead of ApiRoot it is AbiRoot. Fixed the typo and changed it to "3GPP Target SBI ApiRoot wrong syntax".	4	22.4.0
34919648	Timestamp not displayed on "View Handshake Status" page	Two APIs are used to return the handshake status. One API returns the timestamp, other API doesnot returnt he timestamp. Following API for handshake returns timestamp: http://<SEPP_CONFIG:PORT>/sepp-configuration/v1/handshakestatus Following API for handshake status does not return the timestamp: http://<SEPP_CONFIG:PORT>/sepp-configuration/v1/handshakestatus/hostedsepp Fixed the code and handshake status will be returned in both the APIs	4	22.4.0

Table 4-48 (Cont.) SEPP 23.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34892299	Latency metric corrections required in user guide	Document issue: Latency metrics is not having processing time as a parameter, but it is mentioned in the user guide. The SEPP user guide has been updated.	4	22.4.0
34811294	RegExp for Fqdn in body IE needs to be corrected	Regular expression: (?<=http://|https://)[^:/?]+ ========== As per 29.510 reqNfFqdn: $ref: '#/components/schemas/Fqdn' ========== and it does not begin with http or https. The code has been updated to make it compatible with RFC 29510.	4	22.4.0
34806231	Error message not proper if invalid TriggerPoint & Operation is mentioned in header configuration for TH	Proper error message is not being displayed if invalid TriggerPoint and Operation is mentioned in header configuration for topology hiding. Updated the code to display proper error title and cause then can be understandable to user.	4	22.4.0
34805866	Metric ocsepp_topology_body_failure_total user friendly error_msg and missing attribute statusCode	statusCode attribute is missing from metric ocsepp_topology_body_failure_total also the error_msg needs to be formatted. Formatted the error message and added statusCode in the metric.	4	22.4.0
34805800	Missing attribute remote_sepp_name from metric ocsepp_topology_body_success_total	Attribute remote_sepp_name from metric ocsepp_topology_body_success_total is missing. Added remote_sepp_name in ocsepp_topology_body_success_total	4	22.4.0
34800921	Trigger point is displayed blank on CNCC UI for body IE configuration.	Trigger point is displayed blank at CNC Console for body IE configuration. Under Topology Hiding, in Body IE options, check any existing Body IE configurations, the trigger point is displayed as blank. The code has been updated to display the default value for in 'Trigger point' parameter.	4	22.4.0

Table 4-48 (Cont.) SEPP 23.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34745796	Some correction require in Grafana graph heading showing in milli second(ms) and value in traffic instead of second(s)	Some corrections are required in Grafana graph heading, as it was displaying the values in milli second instead of second. 1. CN32F processing time graph heading was showing in ms. 2. PN32F processing time graph heading was showing in ms and value showing in Million (min , max,avg). 3. Ingress Gateway processing time graph heading showing in ms. 4. Egress Gateway processing time graph heading showing in ms. Updated the charts.	4	22.4.0
34724085	TH Error is not proper if the value of enabled is not true/false	Topology Hiding error is not properly displayed if the value of enabled is set to true or false. JSON parse error: Unrecognized token 'TRUE': was expecting (JSON String, Number, Array, Object or token 'null', 'true' or 'false'); nested exception is com.fasterxml.jackson.databind.JsonMappingException: Unrecognized token 'TRUE': was expecting (JSON String, Number, Array, Object or token 'null', 'true' or 'false'). Updated the code to display user readable error.	4	22.4.0
34598843	Format the response for PATCH request in case of failure scenario	Response: Invalid values for field isEnabled is displayed when sent in PATCH request. Allowed values are TRUE OR FALSE Response is not formatted displaying title, status, detail, cause, invalidParams. As a part of fix, the response has been formatted to make it user readable.	4	22.3.0
34597783	Error format not proper if security capability is not TLS/PRINS	Error format is not accurate if the security capability is anything other than TLS/PRINS. Error format should be in the proper format: Title, Cause, Status, Details, InvalidParam, and so on. As a part of the fix, formatted the response and made it user readable.	4	22.3.0
35061921	22.4.x SEPP documentation issues.	There are some documentation gaps in the "Metrics" section of the SEPP User Guide. Updated the SEPP User Guide.	4	22.4.0

Table 4-48 (Cont.) SEPP 23.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35053402	Mediation service default log level shall not be DEBUG	In the default custom yaml of SEPP, mediation service log level is set as DEBUG.	4	22.4.0

> **Note:**
>
> Resolved bugs from 22.4.x have been forward ported to release 23.1.0.

4.2.12 UDR Resolved Bugs

UDR 23.1.3 Resolved Bugs

There are no resolved bugs in this release.

Table 4-49 UDR 23.1.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35152038	Subscribers not migrated when there is a large separation between subs/msisdns numbers.	The subscribers were not migrated to the database when the range between subscribers and Mobile Station Integrated Services Digital Network (MSISDN) numbers was more.	2	22.4.0
35359962	Provgw 'Internal Server Error' while executing GET command using HTTPS	There was Provisioning Gateway Internal Server Error when preforming GET request using HTTPS method.	2	23.2.0
35247269	Migration_Tool in cnUDR doesn't work	Migration tool was not starting because the 4G UDR connection was not correct.	3	23.1.0
35351031	SLF 23.1.1 Update SLF Alert yaml file by removing cndbtier related alert	cnDBTier related alerts were included in the SLF alert yaml file.	3	23.1.1
35356211	Bulk Migration - Schema validation failed.	Schema validation was failing for bulk import migration.	3	23.1.1
35251872	Change the External Traffci Policy on the diam-gateway of the cnUDR	externalTrafficPolicy flag was added in the custom-values.yaml.	3	22.4.0

Table 4-49 (Cont.) UDR 23.1.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35238832	Provisioning of State to VSA in SM-DATA is not increasing ETAG Value	Entity Tag (ETAG) value was not incrementing after provisioning of State to Vendor Specific Attributes (VSA) in SM-DATA.	3	23.1.0
35537442	UDR 23.1.0 Rest API doc mentioning incorrect api prefix for overload	URD REST guide was missing igw-sig and igw-prov in the Rest URL for overload handling.	4	23.1.0

Note:

Resolved bugs from 23.2.0 have been backported to release 23.1.2.

Table 4-50 UDR 23.1.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35171984	UDR 22.4.0: Unable to Delete the Provisioned Subscriber	The delete subscriber operation was not working when UDR was installed in nudr-dr mode.	2	22.4.0
35073690	UDR provisioning with NetCracker is not working after upgrade to 22.4.0	When UDR was upgraded from 22.1.0 to 22.4.0, the UDR provisioning with NetCracker was not working. Ingressgateway displayed the following error: "Internal Server Error".	2	22.4.0
35243257	ETAG Value is not added for signaling PUT after Policy-Data deletion via Provisioning	The ETag value was not attached to the sm-data when policy data was created. This issue is resolved by adding the ETag value for signaling PUT operation.	2	23.1.0
35232485	Entitlement not recognised from cnUDR in 4g PCRF	In the current behavior of diameter interface, all subscriber keys and entitlements are converted to uppercase. UDR behavior is changed to send the entity fields without any case conversion.	2	23.1.0

Table 4-50 (Cont.) UDR 23.1.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35131036	The NULL string is not allowed in an update request, but it is allowed for a create request.	When testing the subscriber UPDATE query using the provisioning gateway (UDR mode) using SOAP request, it is observed that when the custom variable value was set to "NULL" or "null", the request failed with 70015 error. When this value was changed to any other value, such as "NULL1" or "null1", the request was processed.	3	22.4.0
35208993	SLF-ATS 23.1.0_Unable to collect ATS pcap logs	The Helm release name for the SLF and provisioning gateway must not include the ocats keyword. The ATS PcapLog collection feature does not initiate the tcpdump command on the pod that has ocats in its name.	3	23.1.0
35232688	Quota usage for 4G PCRF in cnUDR	In the current behavior, if there is no quota inside the usage, data is not created. The code is fixed to create data with empty usage.	3	23.1.0
35264336	"udr_etag_rest_response_total" Metrics has response Code 201 for GET Request	Incorrect metrics response was observed for the PUT operation. The GET operation metrics counter is getting incremented instead of the PUT operation metrics counter.	3	23.1.0

Table 4-51 UDR 23.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34990450	EIR Allowing update operation for both IMEI and IMEISV for the same user in PUT provisioning	EIR is allowing update for both International Mobile Equipment Identity (IMEI) and International Mobile Equipment Identity – Software Version (IMEISV) for the same user in PUT provisioning. This is a code issue.	2	22.4.0
34861862	UDR is not sending PNR to PCRF for Sh Data Change	Subscribe Notification Request (SNR) for subscriber data is not generating Push Notification Request (PNR) if subscriber data is updated using SOAP/ XML.	2	22.4.0
35019236	cnUDR bulk import does not migrate complete users	The bulk import provisioning is expected to have two state entities. This is a code issue.	3	22.2.3
35012961	nrf-client-mgmt section is not having min and max replicas in yaml	The minimum and maximum replicas are not part of custom.yaml file for nrf-client-mgmt section. This will be exposed in 23.1.0 release.	3	22.4.1
34960248	Prov GW: stale session in db is created if "deleting the only key" is executed and successful with error 0 instead of 70044	You cannot delete the key value for a subscriber present in the database if the subscriber has only one key value.	3	22.4.0
34958407	No alarm/alert is generated for "No disk space for the result log" (EIR.BULKPROV.ALERT .3100)	Alarm and alerts are not generated for "No disk space for the result log" for bulk provisioning as per the requirement "EIR.BULKPROV.ALERT .3100". This is a code issue.	3	22.4.0
34954506	OcudrDbServiceDown " alartm/alert is not displayed in Promethous even after CNDB restart	Alarm and alerts for "OcudrDbServiceDown" are not displayed in Promethous even after Cloud Native Database (CNDB) restarts. This issue requires enhancement in the custom values.yaml file and in the alert files.	3	22.4.0

Table 4-51 (Cont.) UDR 23.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34951275	"OcudrPodsRestart " alarm/alert is not generated for restart of BULK PROV POD	Alarm and alerts for "OcudrPodsRestart" are not generated for restarting of bulk provisioing pod. This requires changes in the Alerts.yaml file.	3	22.4.0
34951074	Unable to edit "PDBI File Expiry Time:" in CCUI GUI	The user is not able to edit the "Provisioning Database In terface (PDBI) File Expiry Time" in the Graphical User Interface (GUI). This is a code issue.	3	22.4.0
34938263	BulkImport migration doesn't support some characters	Bulk migration of subscriber data from 4G UDR to 5G UDR does not support some characters. The regex pattern is changed in 5G UDR as per the 4G UDR to reslove this issue.	3	22.4.0
34937646	EIR Response to GET request on signaling is not correct when default response in dr-service is updated.	For users with incorrect Subscription Permanent Identifier (SUPI) and Generic Public Subscription Identifier (GPSI) the response received for GET request is 200 ok. Since this is a string it will use the values that is configured for defaultResponse.	3	22.4.0
34882819	Config-Server service in SLF is not supporting more than one pod	The config server is not supporting more than one pod in yaml file. The replicas parameter under config-server section is set as 2 to resolve this issue.	3	22.2.1
34866529	EIR 22.3.3 Bulk import not working	During EIR provisioning test using PDBI file, it is found that the log file inside the "/home/udruser/pdbi/" is showing the wrong summary report.	3	22.3.3
34835495	If there are no traces found in jaeger query service, per info service logs has jaeger error	After providing the correct jaeger URL during Helm installation, per-info service logs has jaeger errors when there are no traces present in the jaeger query service.	3	22.4.0

Table 4-51 (Cont.) UDR 23.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34979801	Unable to migrate all subscribers using migration tool (cnUDR)	There is an issue when we define a wide range of Mobile Station Integrated Services Digital Network (MSISDN) to migrate. The migration tool does not support migration of subscriber with only one entity state.	3	22.4.0

Note:

Resolved bugs from 22.3.4 and 22.4.1 have been forward ported to release 23.1.0.

4.2.13 Common Services Resolved Bugs

4.2.13.1 Alternate Route Service Resolved Bugs

Release 23.1.0

There are no resolved bugs in this release.

4.2.13.2 App-Info Resolved Bugs

Table 4-52 App-Info 23.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34851516	Support of supported versions of resources for PDB and HPA in our common services	Warning was observed in logs because of the deprecated version of Kubernetes library used.	3	22.2.0

4.2.13.3 ASM Configuration Resolved Bugs

Release 23.1.0

There are no resolved bugs in this release.

4.2.13.4 ATS Resolved Bugs

Table 4-53 ATS 23.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35077301	Policy ATS behave process is abnormally killed when applogs are set to true.	The ATS behave process is getting terminated when Fetch_log_uplon_failure is set to true in Jenkins. This occurred after implementing the Parallel Execution Framework changes. As a resolution, ATS is deployed with higher footprint, 4 CPU and 6Gi memory.	2	23.1.0

4.2.13.5 Debug Tool Resolved Bugs

Release 23.1.0

There are no resolved bugs in this release.

4.2.13.6 Egress Gateway Resolved Bugs

Release 23.1.0

There are no resolved bugs in this release.

4.2.13.7 Ingress Gateway Resolved Bugs

Release 23.1.0

There are no resolved bugs in this release.

4.2.13.8 Helm Test Resolved Bugs

Release 23.1.0

There are no resolved bugs in this release.

4.2.13.9 Mediation Resolved Bugs

Table 4-54 Mediation 23.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34355757	Issue with Mediation Rule: "add(String path, T value)" body rule api & "del(String path, T value)" header and body rule api	Issue with Mediation Rule: "add(String path, T value)" body rule api & "del(String path, T value)" header and body rule api	3	22.2.0
34459393	Mediation microservice is going in CrashLoopBackOff state after setting LOG_LEVEL in deployment file to RULE_TRAIL	Mediation microservice is going in CrashLoopBackOff state after setting LOG_LEVEL to RULE_TRAIL in deployment file.	3	22.2.1
34348065	When creating mediation rules, SCP does not report correct error details when header or body condition blocks exceed maximum values	When creating mediation rules, SCP does not report correct error details when header or body condition blocks exceed maximum values.	4	22.2.0
34504199	SCP shows inconsistent error details when a mandatory parameter is missing while creating mediation trigger point	SCP shows inconsistent error details when a mandatory parameter is missing while creating mediation trigger point.	4	22.3.0
34487740	SCP displays the incorrect error detail cause when the start range exceeds the end range while creating mediation trigger rule	SCP displays the incorrect error detail cause when the start range exceeds the end range while creating mediation trigger rule.	4	22.3.0

4.2.13.10 NRF-Client Resolved Bugs

Table 4-55 NRF-Client 23.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34767664	Warnings observed while performing Helm Install/Upgrade	Inside nrf-client-nfmanagement/templates/hooks.yaml, SERVICE_MESH_CHECK variable is mentioned twice inside a single block, thus giving a warning while running Helm install command. Duplicated SERVICE_MESH_CHECK variable definitions are removed from file nrf-client-nfmanagement/templates/hooks.yaml in 4 different Jobs.	4	22.3.1
34836483	Add Resource version to HPA/PDB resources while supporting multiple Versions through helm	Upgrade/Rollback fails due to conflict in hpa/pdb resources. When different versions of Kubernetes APIs get created with the same name between upgrades, ApiVersion value like "v1" or "v2beta1" was appended to resource's name to make it different in case apiVersion changes.	2	22.3.0
34647881	Add the minReplicas and maxReplicas for nfmanagement.	Adding HorizontalPodAutoscaler resource for nfmanagement and removeReplicas flag to remove "replicas: " property from NRF-Client deployments (when true) or set it same value as "minReplicas: " property (when false).	2	22.3.0

Table 4-55 (Cont.) NRF-Client 23.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34652873	UDR is going to SUSPEND State after one hour of registration	UDR goes to suspended state after an hour of registration. The problem is 'envMysqlSecondaryHost' environment variable is not defined, therefore, it takes the default value of 'database-mysql' and since that resource is not installed, the error is generated. To fix it, it's not now necessary to define the environment variable 'envMysqlSecondaryHost'.	2	22.3.0
34596069	Nrf-Client-nfmanagment errors impact 100% call failure on nrf-client-discovery pod	Once the Egress Gateway pod enters a non-response state, NrfClient mgmt pods got some error leg, which impacts Nrfdiscovery pods. This leads to 100% call failure for Nrf discovery requests. That is, if NrfMgmt pod , there is 100% failure for discovery requests, which is considered serious.	2	22.3.2
34645097	PCF NRFClient MGMTPod sending intermittent"http2.remote_reset" even with 200 success response	NrfClient mgmt pod is sending "http2.remote_reset" intermittently even with 200 responses.	3	22.4.0
34609875	nrf-client-nfdiscovery shows "Healthy NRF Routes available, cannot send Request"	The nrf-client-nfdiscovery pod cannot reach Healthy NRF Routes available. OCNRF is not able to send Request due to cache management where nrf-route-list is stored.	3	22.3.0
34836499	"envNfNamespace" variable is impacting single NRF-M pod deployment	NfManagement deployment fails due to missing "envNfNamespace" variable, this happens irrespectively of single or multipod deployment.	3	22.3.0

4.2.13.11 Perf-Info Resolved Bugs

Release 23.1.0

There are no resolved bugs in this release.

4.3 Known Bug List

The following tables list the known bugs and associated Customer Impact statements.

4.3.1 BSF Known Bugs

BSF 23.1.4 Known Bugs

There are no new known bugs in this release. Known bugs from 23.1.0 have been forward ported to Release 23.1.4.

BSF 23.1.3 Known Bugs

There are no new known bugs in this release. Known bugs from 23.1.0 have been forward ported to Release 23.1.3.

BSF 23.1.2 Known Bugs

There are no new known bugs in this release. Known bugs from 23.1.0 have been forward ported to Release 23.1.2.

BSF 23.1.1 Known Bugs

There are no new known bugs in this release. Known bugs from 23.1.0 have been forward ported to Release 23.1.1.

Table 4-56 BSF 23.1.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35068048	Alerts on "new state : CONGESTED" and could see OutOfMemoryError on newly added diam-gateway pods	There are alerts on the CONGESTED state and OutOfMemory Error is displayed on newly added diam-gateway pods.	When this issue occurs, the diameter-gateway service does not respond to any other services and it enters the loss of service state. **Workaround**: When this issue occurs, the diameter-gateway service does not respond to any other services and it enters the loss of service state. Restart the diameter-gateway service pod to resolve the issue.	3	22.2.5

4.3.2 CDCS Known Bugs

CDCS Release 23.1.1

There are no known bugs in this release.

CDCS Release 23.1.0

There are no known bugs in this release.

4.3.3 CNC Console Known Bugs

CNC Console 23.1.3 Known Bugs

There are no known bugs in this release.

CNC Console 23.1.2 Known Bugs

There are no known bugs in this release.

CNC Console 23.1.1 Known Bugs

There are no known bugs in this release.

Table 4-57 CNC Console 23.1.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35106559	Console enhancement needed to access Promxy GUI	Promxy API access works seamlessly through Console but the user must append "/graph" manually to access the GUI.	No customer impact **Workaround**: On selecting Promxy from Console, the user must append "/graph" to the url to access the GUI. For example: https://<CNCC IP/FQDN:PORT>/<cluster name>/promxy/graph	4	22.3.1

4.3.4 cnDBTier Known Bugs

cnDBTier Release 23.1.3

Table 4-58 cnDBTier 23.1.3 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35848919	Connectivity fails towards "running" ndbappmysqld pods' mysql-server during upgrade. Behaviour not seen during pod termination.	ndbappmysqld pods move to the running status before the mysql process is ready.	During a rolling restart of ndbappmysqld pods, two ndbappmysqld pods may not get connected to the NF application through the connectivity service at the same time leading to potential traffic loss. **Workaround**: Configure more than two ndbappmysqld pods while performing a rolling restart of ndbappmysqld pods to ensure that there are operational pods to manage the incoming traffic.	2	23.3.0

cnDBTier Release 23.1.2

Table 4-59 cnDBTier 23.1.2 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35848919	Connectivity fails towards "running" ndbappmysqld pods' mysql-server during upgrade. Behaviour not seen during pod termination.	ndbappmysqld pods move to the running status before the mysql process is ready.	During a rolling restart of ndbappmysqld pods, two ndbappmysqld pods may not get connected to the NF application through the connectivity service at the same time leading to potential traffic loss. **Workaround**: Configure more than two ndbappmysqld pods while performing a rolling restart of ndbappmysqld pods to ensure that there are operational pods to manage the incoming traffic.	2	23.3.0
35590372	cnDBTier 23.2.0 MIBs and alertrules don't match	cnDBTier 23.2.0 Management Information Base (MIBs) and alertrules are not matching.	The module identity defined in the MIB template doesn't match with the Object Identifiers (OIDs) of the alerts. As a result, Simple Network Management Protocol (SNMP) is unable to trap any alert raised by the system leading to missing traps that are collected. **Workaround**: Before installing or upgrading cnDBTier, perform the following steps: • Update the configuration in `occndbtier_mib.mib`: 1. Open the `occndbtier_mib.mib` file in the `<CSAR_FILE_EXTRACTED>/Artifacts/Scripts/snmp_mibs` folder. 2. Update the configuration in line number "44" from `::= { oracleDbTier 2 }` to `::= { oracleDbTier 1 }` • Update the configuration in `occndbtier_mib_tc.mib`: 1. Open the `occndbtier_mib_tc.mib` file in the `<CSAR_FILE_EXTRACTED>/Artifacts/Scripts/snmp_mibs` folder. 2. Update the configuration in line number "43" from `::= { oracleDbTier 2 }` to `::= { oracleDbTier 1 }`	3	23.2.0

Table 4-59 (Cont.) cnDBTier 23.1.2 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35734862	Helm chart takes wrong startNodeId for ndbmysqld from custom values.yaml	Helm chart picks incorrect `startNodeId` value for the `ndbmysqld` pod from the `custom values.yaml` file.	The replication SQL pod reads the node ID that belongs to the APP pod. Therefore, if the APP pod is not present for the specified node, then the `init` container of the replication SQL pod doesn't come up. **Workaround**: Before installing or upgrading cnDBTier, perfrom the following steps to update the `sts.yaml` file: 1. Open the `sts.yaml` file in the `occndbtier/charts/api/templates/` folder. 2. Update the configuration in line number "505" from `value: {{ .Values.global.ndbapp.startNodeId | default 70 | quote }}` to `value: {{ .Values.global.api.startNodeId | default 56 | quote }} .`	3	23.1.2

cnDBTier Release 23.1.1

Table 4-60 cnDBTier 23.1.1 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35139386	During CNDB upgrade from 22.4.1 to 23.1.0, multiple restarts can be observed in ndbmysql pods	Rotation of general query log on replication SQL pod is not working leading to continuous restart of container.	MySQL Replication pods restarts continuously due to general query log purge issue. **Workaround:** Before installing or upgrading cnDBTier, disable the general query log feature by setting the `general_log` parameter to `OFF` (`general_log: 'OFF'`) in the `/global/api` section of the `custom_values.yaml` file.	1	23.1.1

Table 4-60 (Cont.) cnDBTier 23.1.1 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35848919	Connectivity fails towards "running" ndbappmysqld pods' mysql-server during upgrade. Behaviour not seen during pod termination.	ndbappmysqld pods move to the running status before the mysql process is ready.	During a rolling restart of ndbappmysqld pods, two ndbappmysqld pods may not get connected to the NF application through the connectivity service at the same time leading to potential traffic loss. **Workaround**: Configure more than two ndbappmysqld pods while performing a rolling restart of ndbappmysqld pods to ensure that there are operational pods to manage the incoming traffic.	2	23.3.0
35734862	Helm chart takes wrong startNodeId for ndbmysqld from custom values.yaml	Helm chart picks incorrect `startNodeId` value for the `ndbmysqld` pod from the `custom values.yaml` file.	The replication SQL pod reads the node ID that belongs to the APP pod. Therefore, if the APP pod is not present for the specified node, then the `init` container of the replication SQL pod doesn't come up. **Workaround**: Before installing or upgrading cnDBTier, perfrom the following steps to update the `sts.yaml` file: 1. Open the `sts.yaml` file in the `occndbtier/charts/api/templates/` folder. 2. Update the configuration in line number "489" from `value: {{ .Values.global.ndbapp.startNodeId | default 70 | quote }}` to `value: {{ .Values.global.api.startNodeId | default 56 | quote }} .`	3	23.1.2

cnDBTier Release 23.1.0

Table 4-61 cnDBTier 23.1.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35139386	During CNDB upgrade from 22.4.1 to 23.1.0, multiple restarts can be observed in ndbmysql pods	Rotation of general query log on replication SQL pod is not working leading to continuous restart of container.	MySQL Replication pods restarts continuously due to general query log purge issue. **Workaround:** Disable General Query Log feature by setting the `general_log` parameter to `OFF` (`general_log: 'OFF'`) in the `/global/api` section of the `custom_values.yaml` file.	1	23.1.0
35125409	Replication breaks and same error observed in ndbmysql pod in two scenarios - MTA feature is not working	Georeplication breaks on MTA enabled cnDBTier setups, therefore MTA feature has to be disabled.	Georeplication established between cnDBTier sites breaks with the "coordinator stopped" error. **Workaround:** Disable MTA feature by setting the `replica_parallel_workers` parameter to "`0`" ("`replica_parallel_workers: 0`") in the `/global/additionalndbconfigurations/mysqld` section of the `custom_values.yaml` file.	2	23.1.0

35217746	NRF 23.1 cnDBTier Rollback Failure	Rollback fails while running the `hooks.sh --post-rollback` script from Bastion Host.	Rollback without service account from cnDBTier version 23.1.x to 22.4.x fails.
			Workaround:
			Run the following commands before running "`occndbtier/files/hooks.sh --post-rollback`" when rolling back from cnDBTier 23.1.0 (NDB Version: 8.0.32) to cnDBTier 22.4.2 (NDB Version: 8.0.31):
			
			`export from_version=8.0.32`
			`export to_version=8.0.31`
			`sed -i '/.*to_version=$(mysqlver)/s/^/#/g' occndbtier/files/hooks.sh`
			`sed -i '/.*from_version=$(mysqlver)/s/^/#/g' occndbtier/files/hooks.sh`
				2	23.1.0, 22.4.0, 22.4.1

Table 4-61 (Cont.) cnDBTier 23.1.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35848919	Connectivity fails towards "running" ndbappmysqld pods' mysql-server during upgrade. Behaviour not seen during pod termination.	ndbappmysqld pods move to the running status before the mysql process is ready.	During a rolling restart of ndbappmysqld pods, two ndbappmysqld pods may not get connected to the NF application through the connectivity service at the same time leading to potential traffic loss. **Workaround**: Configure more than two ndbappmysqld pods while performing a rolling restart of ndbappmysqld pods to ensure that there are operational pods to manage the incoming traffic.	2	23.3.0

4.3.5 CNE Known Bugs

CNE 23.1.4 Known Bugs
There are no known bugs in this release.

CNE 23.1.3 Known Bugs
There are no known bugs in this release.

Table 4-62 CNE 23.1.2 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
34978552	After Upgrade to 22.3 VMware LBs are left with dysfunctional ifcfg file	After CNE upgrade on VMware cluster, most of the STANDBY LBs and several ACTIVE LBs are left with a dysfunctional /etc/sysconfig/networking-scripts/ifcfg-ens192 file.	After an upgrade, during a Load Balancer VM (LBVM) switchover, the current VMware version requires VMs to reboot to remove the active interfaces and make the new ones active. This behavior leads to several interfaces, that were supposed to be deleted from configuration file, to remain active leaving the cluster in a failed state. **Workaround**: Manually configure LBVM configuration files to point to the correct interfaces.	2	22.4.0
35089494	Opensearch Index Management Operations are not working	Opensearch Index management operations are failing: indexes are not transitioning from hot to warm state, and force merge and delete are not working for any indexes.	Entire Index management lifecycle fails. **Workaround**: Manually invoke curl requests, and force merge and delete indexes periodically.	2	23.1.1

Table 4-62 (Cont.) CNE 23.1.2 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35182156	LBVMs unable to communicate with backend services	Load Balancer Virtual Machines (LBVM) are unable to communicate with the backend services as the k8s Security Group (SG) overrides the k8s_node_secgroup SG. To overcome this issue, both the k8s and k8s_node_secgroup SGs, that are applied to worker nodes, must be combined.	When there are two SGs that are used in the same node, one SG overrides the other SG as per the rules applied. Therefore, the rules go missing and node communication does not work. **Workaround**: Manually add the rules needed at the OpenStack desktop.	2	22.4.1
35168065	High CPU usage on CNE 22.4.1 nodes	Individual master nodes are showing High CPU usage while other master nodes have very low usage.	One of the master nodes in quorum of three shows high CPU usage and causes performance concerns. **Workaround**: Manually change egress controller configmap values and perform rolling restart of Egress controller pods. For more information, see "*Verifying LBVM HTTP Server*" in *Oracle Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide*.		

Table 4-63 CNE 23.1.1 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
34978552	After Upgrade to 22.3 VMware LBs are left with dysfunctional ifcfg file	After CNE upgrade on VMware cluster, most of the STANDBY LBs and several ACTIVE LBs are left with a dysfunctional /etc/sysconfig/networking-scripts/ifcfg-ens192 file.	After an upgrade, during a Load Balancer VM (LBVM) switchover, the current VMware version requires vms to reboot to remove the active interfaces and make the new ones active. This behavior leads to several interfaces, that were supposed to be deleted from configuration file, to remain active leaving the cluster in a failed state. **Workaound**: Manually configure LBVM configuration files to point to the correct interfaces.	2	22.4.0
35089494	Opensearch Index Management Operations are not working	Opensearch Index management operations are failing: indexes are not transitioning from hot to warm state, and force merge and delete are not working for any indexes.	Entire Index management lifecycle fails. **Workaround**: Manually invoke curl requests, and force merge and delete indexes periodically.	2	23.1.1

Table 4-63 (Cont.) CNE 23.1.1 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35182156	K8s and k8s-node SGs should be combined	Request to combine the Kubernetes and k8s-node Security Groups (SGs) that are applied to worker nodes.	When there are two SGs that are used in the same node, one SG overrides the other SG as per the rules applied. Therefore, there rules go missing and node communication does not work. **Workaround**: Manually add the rules needed at the openstack desktop.	2	22.4.1
35168065	High CPU usage on CNE 22.4.1 nodes	CNE traffic is not evenly distributed across control nodes. As a result, the CPU usage of one control node is extremely high and other control nodes is negligible	Particular master node shows high CPU usage causing performance concerns. **Workaround**: Manually change the egress controller configmap values and perform rolling restart of Egress controller pods after installation or upgrade. For detailed steps, see the "Performing a Control Plane Patch" section in *Oracle Communication Cloud Native Environment Installation Guide* and *Oracle Communication Cloud Native Environment Upgrade Guide*.	2	22.4.1

Table 4-63 (Cont.) CNE 23.1.1 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
34686444	Both LBVMs for a service going down at the same time corrupts the SQL database on the lb-controller	SQL database containing the information about which LBVM is active and which LBVM is standby for a particular service is populated with FAILED entries.	Cluster communication over HAProxy handler doesn't get a reply. As a result, the runCmd throws a RuntimeError that is not caught and terminates the monitor. **Workaround**: Manually perform a recover to ACTIVE/UP and STANDBY/UP states on LBVM nodes.	3	• 22.4.0 • 1.10.3

Table 4-64 CNE 23.1.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35061535	Intermittently Fluent Bit fails to ingest logs certain data types	During the log forwarding process in FluentBit, in some case, it is observed that FluentBit stalls to ingest data in OpenSearch. During the issue investigation, it is found that the source of the issue is the OpenSearch index creation process. OpenSearch index creation process blocks (indexblock) ingestion API calls when the cluster observes high disk usage or high compute usage, leading to HTTP 403 errors.	Delay in seeing the logs or no logs are seen in the OpenSearch dashboard. **Workaround**: Perform the following steps to fix HTTP 403 exception: 1. Log in to OpenSearch dashboard and its console (*http://<LOAD_BALANCER_IP>/<CLUSETER_NAME>/dashboard/app/dev_tools#/console)* 2. Run the following command to fix the exception: `PUT /_all/_settings {"index.blocks.read_only_allow_delete": null,"index.blocks.write": null}` Perform the following steps to fix mapper_parsing_exception:	2	23.1.0

Table 4-64 (Cont.) CNE 23.1.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
			1. Use SSH to log in to the Bastion Host 2. Run the following command to edit the configmap: `kubectl -n occne-infra edit cm occne-fluent-bit` 3. Edit the configmap entry in the FILTER section and turn off Annotations and Labels: *[FILTER]* *Name kubernetes* *Match kube.** *Merge_Log On* *Merge_Log On* ***Annotations Off*** ***Labels Off*** *K8S-Logging.Parser On* *K8S-Logging.Exclude On* 4. Run the following command to		

Table 4-64 (Cont.) CNE 23.1.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
			recycle the pods: `kubectl delete pods -n occne-infra -l app.kubernetes.io/name=flu ent-bit`		
35089494	Opensearch Index Management Operations are not working	Opensearch Index management operations are failing. Indexes are not transitioning from hot to warm state. Force merge and delete is not working for any indexes.	Entire Index management lifecycle fails. **Workaround**: Manually invoke curl requests, force merge, and delete indexes periodically.	2	23.1.0
34686444	Both LBVMs for a service going down at the same time corrupts the SQL database on the lb-controller	SQL database containing the information about the LBVM status (active and standby LBVM) for a particular service populates with FAILED entries.	Cluster communication over HAProxy handler doesn't get a reply and runCmd throws a RuntimeError that is not caught and the monitor is killed. **Workaround**: Manually perform a recovery to update the ACTIVE/UP and STANDBY/UP states on the LBVM nodes.	3	1.10.3 22.4.0

Table 4-64 (Cont.) CNE 23.1.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35168065	High CPU usage on CNE 22.4.1 nodes	CNE traffic is not evenly distributed across control nodes. As a result, the CPU usage of one control node is extremely high and other control nodes is negligible	Particular master node shows high CPU usage causing performance concerns. **Workaround**: Manually change the egress controller configmap values and perform rolling restart of Egress controller pods after installation or upgrade. For detailed steps, see the "Performing a Control Plane Patch" section in *Oracle Communication Cloud Native Environment Installation Guide* and *Oracle Communication Cloud Native Environment Upgrade Guide*.	2	22.4.1

4.3.6 NEF Known Bugs

NEF Release 23.1.4

There are no known bugs in this release.

NEF Release 23.1.3

There are no known bugs in this release.

NEF Release 23.1.2

There are no known bugs in this release.

NEF Release 23.1.1

There are no known bugs in this release.

NEF Release 23.1.0

There are no known bugs in this release.

4.3.7 NRF Known Bugs

NRF 23.1.4 Known Bugs

There are no known bugs in this release. For existing known bugs, see Table 4-65.

NRF 23.1.3 Known Bugs

There are no known bugs in this release. For existing known bugs, see Table 4-65.

NRF 23.1.2 Known Bugs

There are no known bugs in this release. For existing known bugs, see Table 4-65.

NRF 23.1.1 Known Bugs

There are no known bugs in this release. For existing known bugs, see Table 4-65.

Table 4-65 NRF 23.1.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
34844121	NRF Auditor: Install hook and auditor service are taking leaderElectionDbName from different places	Install hook and auditor service are taking leaderElection DbName from different places. Hooks area which is install is taking leaderElection DbName from secret but Auditor logic is taking db name from values.yaml.	While configuring secrets leaderElection DbName value shall match with global.database.leaderElectionDbName in custom values.yaml, otherwise Auditor microservice will not come up. **Workaround**: A note is added in Oracle Communications Cloud Native Core, Network Repository Function Installation, Upgrade, and Fault Recovery guide to match the leaderElection DbName value in secret with global.database.leaderElectionDbName in custom values.yaml file used for deployment.	3	22.3.1

Table 4-65 (Cont.) NRF 23.1.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
34986707	ocnrf_replication_status_check_total does not get scraped from the artisan pod	ocnrf_replication_status_check_total does not get scraped from the artisan pod. OcnrfReplicationStatusMonitoringInactive alert will be raised for the pod.	OcnrfReplicationStatusMonitoringInactive alert will be raised for the pod. **Workaround**: Update the alert expression to exclude nrfartisan service like below: sum by(pod) (irate(ocnrf_replication_status_check_total{container!~"nrfauditor|nrfartisan" }[5m])) == 0	3	22.3.2
34205871	3gpp-Sbi-Correlation-Info header not populated in response generated from IGW and NRF microservices framework	3gpp-Sbi-Correlation-Info header not populated in response generated from IGW and NRF microservices framework.	It can occur in rainy day/ overload cases. **Workaround**: No workaround available	4	22.2.0

Table 4-65 (Cont.) NRF 23.1.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
34205684	OCNRF Preferred locality in NFDiscovery query attributes values having plus symbol or space is generating null pointer in NRF Forwarding use-cases	NRF Preferred locality in NFDiscovery query attributes values having plus symbol or space is generating null pointer in NRF Forwarding usecases.	This issue can occur with any attribute in NFDiscovery query and this is applicable to Roaming scenarios too. NRF forwarding fails with attribute values with space or + characters. **Workaround**: NFDiscover service operation query shall not have space or + symbol in any attribute value to avoid this.	4	22.2.0

Table 4-65 (Cont.) NRF 23.1.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
33894008	NFService level load is not used for calculating NF's load for discoveryResultLoadThreshold feature when Discovery Query is with service-names query parameter having one service in it.	When Discovery query is having service-names query parameter having one service in it, then during load calculation, for discoveryResultLoadThreshold, NRF should consider the NFService level load, if present, else, it will consider NFProfile level load, if present, else , it will use default configured load (defaultLoad). But NRF is not considering the calculated load for discoveryResultLoadThreshold feature when profile load is null and there is one service with load If discoveryResultLoadThreshold feature is disabled, (value as 0), this issue is not observed.	For Discovery query for a single service, NRF will start using the configured defaultLoad for applying discoveryResultLoadThreshold feature even if load is present in NFService. **Workaround**: None, this issue occurs only, discoveryResultLoadThreshold feature is enabled.	4	1.15.0

4.3.8 NSSF Known Bugs

Table 4-66 NSSF 23.1.2 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35183920	Ingress pod memory gradually increasing while running traffic with 2.5K tps with NSSF 23.1.0	During a long performance run of 12 to 14 hours, an increase in RAM utilization was observed at NsSelection Ingress Gateway, impacting the most heavily trafficked Microservices (MS).	The increase in memory utilization is not significant and remains under control. **Workaround**: No workaround available	3	23.1.0
35035379	While adding the Amf-set in CNCC UI, OCNSSF send multiple unknown Headers in discovery message request towards NRF	Based on the operator's configuration, NSSF sent an on-demand Discovery and Subscription to NRF. The issue arose in PCAP logs where many unknown headers were observed. The message was normal until it reached Egress Gateway, but the messages going out through the Egress Gateway had these headers.	There is no impact on the service as NRF successfully processes the message and subscriptions. Additionally, this issue is not reproducible in the development setups but is observed in one of the SPAD setups. **Workaround**: No workaround available	3	22.4.2

Table 4-66 (Cont.) NSSF 23.1.2 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35273531	Operator configured data should not deleted and added while ns-availability update received from AMF	The configuration was getting deleted and recreated in scenarios where there were multiple NsAvailability PUT requests.	The transient requests that occurred during the duration when the old configuration was deleted and the new configuration was inserted were not responded to, considering that configuration. The NsAvailability PUT implementation has been designed to delete the existing availability data and then create a new PUT. **Workaround**: No workaround available	3	23.1.0

Table 4-67 NSSF 23.1.1 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35218657	422 UNPROCESSABLE_ENTITY - when Nokia AMF sends a huge nnssf-nssaiavailability request	Intermittently, NSSF is responding with 422 ERROR response for NsAvailability PUT request. The latency of request processing is high.	The service is getting impacted. This issue is happening intermittently and also for long messages. **Workaround**: Check if there are any database restarts or any logs for connection impairment.	2	23.1.0

Table 4-67 (Cont.) NSSF 23.1.1 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35183920	Ingress pod memory gradually increasing while running traffic with 2.5K tps with NSSF 23.1.0	Ingress pod memory gradually increases while running traffic with 2.5K TPS.	In the long run of performance testing, post 12 to 14 hours, an increase in RAM utilization is observed at NsSelection Ingress Gateway. **Workaround**: The increase in memory utilization is not steep and is under control.	3	23.1.0
35123768	OCNSSF send multiple unknown Headers in subscription message request towards NRF	Based on the operator configuration, NSSF sends an on-demand Discovery and Subscription to NRF. The issue is in PCAP logs as many unknown headers are being seen. The message is intact until it reaches the Egress Gateway (EGW), but the messages that come out of EGW have these headers.	No impact on service as NRF is processing the message, and subscriptions are successful. This issue is not being reproduced in dev setups but is being observed in one of the SPAD setups. **Workaround**: No workaround available	3	23.1.0
35180629	If plmn level Profile is not configured, NS-Availability update failed in first execution after that it works as expected	Intermittently, the NsAvailability request is responding with 200 OK instead of 503 Incomplete Configurations.	Minimal impact as this scenario is not getting replicated in any dev setups. **Workaround**: No workaround available	3	23.1.0

Table 4-67 (Cont.) NSSF 23.1.1 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35265874	Notification not coming to AMF Stub when a particular range is subscribed before configuration	Intermittently, when notification triggers Configuration update and Subscription for the same TAI Range, the notification is not generated from the NsSubscription service.	This issue is a corner case scenario which acts as a subscription and notification trigger using the exact same TAI range. This is an intermittent issue. **Workaround**: No workaround available	3	23.1.0
35261720	NSSF - namespace name is hardcoded in the nssf-alert-rules.yaml	The namespace is hard-coded in the ocnssf-22.4.3.0.0.alert-rules.yaml. There are multiple entries of the hard-coded namespace value “*ocnssf*”, and each entry needs to be edited before deployment in any environment.	Manual update is required. **Workaround**: The operator has to update (replace) ocnssf with the namespace where the deployment exists.	3	22.4.3
35259920	While running 10k traffic with at NSSF with ASM 503 responses are being observed	While running 10K traffic at NSSF with ASM 503 responses are being observed.	Approximately .01% of the traffic is impacted. This issue is being observed intermittently and only while testing with ASM. **Workaround**: No workaround available	3	23.1.0

Table 4-67 (Cont.) NSSF 23.1.1 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35180218	NS selection is not providing correct information just after ns-availability update	NsSelection uses the database to compute the Network Slice Instance during a PDU establishment.NsAvailability service, specifically NsAvailability Update from AMF, is used to update the configuration, which updates the S-NSSAI supported in a TAI.	In a scenario where multiple AMFs update the database, there is a specific window where the configuration gets updated. During this time, NsSelection call is impacted as NsSelection is a GET query, and it takes the read lock while NsAvailability goes into a write lock. **Workaround**: No workaround available	3	23.1.0
35035379	while adding the Amf-set in CNCC UI, OCNSSF send multiple unknown Headers in discovery message request towards NRF	Based on the operator configuration, NSSF sends an on-demand Discovery and Subscription to NRF. The issue is in PCAP logs as many unknown headers are being seen. The message is intact until it reaches Egress Gateway (EGW) but the messages that come out of EGW have these headers.	No impact on service as NRF is processing the message and subscriptions are successful. The issue is not being reproduced in dev setups but is being observed in one of the SPAD setups. **Workaround**: No workaround available	3	22.4.2

Table 4-67 (Cont.) NSSF 23.1.1 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35154193	NSSF and CNDB Tier Communications link failure	NSSF microservices get an exception that occurs due to a communication link issue with cnDBTier. The services on both the back end and cnDBTier look proper.	There has been no traffic loss, as we have observed this exception in logs. But excessive logging can impact traffic, this issue is being analyzed for the root cause. **Workaround**: No workaround available	3	23.1.0
35185702	NsAvailability is creating a duplicate subscription	NsAvailability is creating a duplicate subscription. The criteria for the uniqueness of a subscription is: • Notification URL • Tai List • SiteId (In DB) Ns Availability must not create more than one entry for a Subscription at a given site. The combination of Notification URL and TAI or `TaiRangeList` must be unique in tables. The issue happens when multiple patches on the same subscription come at once.	Minimal impact on traffic as an additional record is inserted only in a rare scenario. **Workaround**: No workaround available	3	23.1.0

Table 4-67 (Cont.) NSSF 23.1.1 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35273531	Operator configured data should not deleted and added while ns-availability update received from AMF	The transient requests that occur when the old configuration is deleted and the new configuration is inserted, do not respond to that configuration.	Configuration gets deleted and recreated in scenarios when there are multiple NsAvailability PUT requests. **Workaround**: NsAvailability PUT implementation is done to delete the existing Availability Data and to trigger a PUT request.	3	23.1.0
35208077	Selection pod memory gradually increasing while running traffic with 2.5K tps with NSSF 23.1.0	Selection pod memory gradually increases while running the traffic with 2.5K TPS.	On a long run of performance testing for 12 to 14 hours, there is an increase in RAM utilization at NsSelection Ingress Gateway. The increase in memory utilization is not steep and is under control. **Workaround**: No workaround available	4	23.1.0

Table 4-68 NSSF 23.1.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35133188	In service upgrade to NSSF 23.1.0 is not supported in NSSF	In service upgrade to NSSF 23.1.0 is not supported in NSSF	In service upgrade would not be supported in this release. **Workaround**: A workaround procedure or MOP can be provided to enable a rolling upgrade. Contact OCC or MOS to request the MOP. This procedure will entail the following steps: 1. Pause traffic 2. Alter Char set for all tables in ProvisionDb and State DB in 22.4.x release schema. 3. Alter State DB tables to add unique constraint and foreign key in 22.4.x release schema. 4. Validate updates. 5. Run a Helm upgrade to 23.1.x	2	23.1.0

Table 4-68 (Cont.) NSSF 23.1.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35114407	10K TPS has glitches when ASM/mTLS is enabled on dbtier	NSSF must support 10k TPS with ASM, but it is not supported in certain scenarios.	With ASM, NSSF can support 7.5k traffic. When 10k traffic is sent, it creates high latency and NSSF responds 5xx for long runs. **Workaround**: No workaround available	3	23.1.0
35095820	IN NSI Profile, NRF Access Token URI is mandatory parameter in CNCC UI	In CNCC UI for NSI Profile, NRF Access Token URI is showing as optional, but it should be mandatory.	API call fails in certain scenarios when the mandatory parameter is not passed. **Workaround**: No workaround available	3	22.4.2
35052539	NSSF is not sending the expected data for log level	CNCC UI is not showing any default log level for all NSSF services.	The customer will not be able to get the log level of all NSSF services from CNCC GUI. **Workaround**: No workaround available	3	22.4.2
35035379	while adding the Amf-set in CNCC UI, OCNSSF send multiple unknown Headers in discovery message request towards NRF	While adding the amf-set in CNCC UI, NSSF sends a discovery message to NRF to get all active AMFs in an AMF-set. In this discovery message request, there are multiple unknown headers.	The customer will not be able to get the log level of all NSSF services from CNCC GUI. There can be an issue for customers who are not using NRF, during the interop scenario if NRF rejects the request because of unexpected headers. **Workaround**: No workaround available	3	22.4.2

Table 4-68 (Cont.) NSSF 23.1.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35022513	NSSF is sending incorrect targetNfType in discovery message towards NRF	In custom values yaml, enable subscription for NRF. As per the logs, NSSF is sending an incorrect targetNfType discovery message to NRF.	Customer impact is minimal as there is no loss of traffic.At the start-up, NSSF sends a discovery message to NRF for NfType AMF intermittently the nftype is not getting a proper value. **Workaround**: No workaround available	3	22.4.2
34874721	NSSF ATS 22.3.0 Health check failure	The health check test in ATS is failing for release 22.3.0.	Customer impact is minimal as there is no loss of traffic. NSSF CNC ATS heath check is getting failed in spite of pods coming up. **Workaround**: No workaround available	3	22.3.0
35036358	Discovery and subscription Message Request and Response should be printed relevant DEBUG log information in OCNSSF	As per the current logs, the user is unable to get the clarity for discovery and subscription requests and responses in logs. Debug log is not printing the relevant log info needed.	Customer impact is very low. Customers won't be able to check the response JSON message in success scenarios. **Workaround**: No workaround available	4	22.4.2

4.3.9 Policy Known Bugs

Policy 23.1.8 Known Bugs

There are no new known bugs for this release. The known bugs from 23.1.x have been forward ported to release 23.1.8.

Table 4-69 Policy 23.1.7 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release

35692751	app-info-infra-check job failing due to pkill error causes the policy installation failure	There is an issue while upgrading from 23.1.6 to 23.1.7 when enabling the hook validation parameters in the *custom.yaml* file.	Policy installation fails due to *app-info-infra-check* job failure.
			Workaround: The following parameters from custom.yaml file should to be left with default value as "false" and upgrade or installation should be performed:
			`hookValidation:`
			`dbSchemaValidate: 'false' # flag to enable pre-flight DB checks for pre-install, pre-upgrade and post-upgrade`
			`infraValidate: false # flag to enable infra-validation check for pre-install and pre-upgrade`
				2	23.1.7

> **Note:**
>
> The known bugs from 23.1.x have been forward ported to release 23.1.7.

Policy 23.1.6 Known Bugs

There are no new known bugs for this release. The known bugs from 23.1.5 have been forward ported to release 23.1.6.

Table 4-70 Policy 23.1.5 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35323283	Stale session - SM sessions are not audited after enabling the Audit from PCF GUI	SM service audit is not scheduled even after enabling it from PCF GUI.	If SM sessions audit enabling fails, then stale SM sessions can get created due to non-audit of the SM session records. **Workaround**: While enabling the audit for SM Policy Association from PCF GUI, toggle the **Audit Enabled** switch twice and click **Save** to enable audit. You can verify the SM service that has registered with the audit service through the audit table.	4	23.1.0

> **Note:**
>
> The known bugs from 23.1.4 have been forward ported to release 23.1.5.

Policy 23.1.4 Known Bugs

There are no new known bugs for this release. The known bugs from 23.1.3 have been forward ported to release 23.1.4.

Policy 23.1.3 Known Bugs

There are no new known bugs for this release. The known bugs from 23.1.2 have been forward ported to release 23.1.3.

Table 4-71 Policy 23.1.2 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35248922	Traffic getting rejected with Error Timeout processing for event: Latency: 4173ms\nDiameter :Sent	The traffic is getting rejected with error timeout processing for the event: Latency: 4173ms\nDiameter:Sent.	When diameter connection is added and removed on diameter gateway, the same information gets stored in distributed cache. Sometimes, this information becomes stale, and it is not updated on diameter connection termination. This may cause some unsolicited diameter messages (RAR and ASR) not getting routed properly to DSRs or DRAs. **Workaround**: The user needs to find out the diameter gateway pods that are giving stale connection information and restart them.	2	22.4.5
35280823	PCF High CPU utilization observed in HPA output for Audit service (47%) with Max Replicas Used	Audit service is running with high CPU utilization and maximum number of replicas even when there are fewer calls being made.	Audit Notifications might get delayed once the CPU utilization is higher. **Workaround**: Set these values in the deployment file of audit service as: • NOTIFY_THREAD_POOL_COUNT: 3 • AUDIT_THREAD_POOL_COUNT: 3 And, set the requested CPU limit to 2.	2	23.1.1
35266983	PCF sends N1N2Subscription every time when PCF attempts to send URSP rule	PCF sends N1N2Subscription every time when PCF attempts to send URSP rule.	The UE service is doing N1N2 subscription twice which as per the specifications should occur once. **Workaround**: The user needs to update policy in such a way that the underlined issue of no UPSI rule to be sent does not occur. In Policy Block, instead of sending UPSI as an Empty List, the user should avoid using Install UPSI Blockly.	2	22.4.1

Table 4-71 (Cont.) Policy 23.1.2 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35308123	Unable to Create multiple tables using Table Slicing	User is unable to create multiple tables using table slicing.	Table Slicing cannot be enabled. **Workaround**: For each slice created for SmPolicyAssociation table, the user needs to add the COMPRESSION_SCHEME column. ALTER TABLE <Database.tableName> ADD COMPRESSION_SCHEME tinyint;	2	23.1.2

Note:

The known bugs from 23.1.1 have been forward ported to release 23.1.2.

Table 4-72 Policy 23.1.1 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35066567	During Upgrade of PCF from 22.3.2 to 22.4.0 Encountered HPA Utilization increased to 90% for PDS services & Max processing time for pds increased to 5s	During the upgrade, HPA utilization of PDS is increased to 91% and maximum processing time for PDS increased to 5s.	During in-service upgrade, timeouts were observed in PDS call processing. **Workaround**: Change the default value of `maxUnavailable` Helm parameter from 50% to 20%.	3	22.4.0

Note:

The known bugs from 23.1.0 have been forward ported to release 23.1.1.

Table 4-73 Policy 23.1.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
34881560	Perf-Info microservice not behaving as expected (CPU usage is beyond the L1 level)	Perf-Info microservice is not behaving as expected. The CPU usage is beyond the L1 level.	When load levels are not published, the associated discard policy/error profiles are not triggered even if the system is under L1/L2/L3 load. **Workaround**: Restart performance pods and reapply overload threshold configuration.	2	22.4.0
35016966	DB Replication goes down while Upgrading PCF application from 22.1.1 to 22.3.3	DB Replication goes down while upgrading PCF application from 22.1.1 to 22.3.3.	When an upgrade was made, the traffic began to fail because the default settings were turned off. Since cmservice does not refresh the saved data during the upgrade and the flag introduced in version 22.4.0 are new, which are by default 'off'. **Workaround**: Add the new flags through the hooks and send it as active, so when the upgrade is done, the existing information will be validated and if queryUserOnCreate is true, then set amPolicyDataEnabled as true. It is applicable for AMService and UEService.	2	22.3.3

Table 4-73 (Cont.) Policy 23.1.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
34596793	ocpm.cne.gateway.exception.EgwCustomException: 400 BAD_REQUEST "unknown protocol: null" observed for nbsf-mgmt scope.	ocpm.cne.gateway.exception.EgwCustomException: 400 BAD_REQUEST "unknown protocol: null" is observed for nbsf-mgmt scope.	Binding to BSF communication fails. **Workaround**: Stop sending this header if the host and port extracted from BSF URL are NULL, even if the flag is set to true.	2	22.2.0
35071996	Susbscriber variable not working as expected	Subscriber variable is not working as expected.	It is not possible to save non-string variables inside state variables. **Workaround**: Use string variables inside state variables instead of non-string variables.	3	22.4.1
35068048	Alerts on "new state : CONGESTED" and could see OutOfMemoryError on newly added diam-gateway pods	There are alerts in the CONGESTED state and OutOfMemoryError is displayed on newly added diam-gateway pods.	When this issue happens the diameter-gateway service does not respond with any other services and it enters the loss of service state. **Workaround**: Increase the Reconnect Delay (sec) value using the CNC Console to resolve this issue. The recommended value is 9 seconds. Restart the diameter-gateway service pod to resolve the issue.	3	22.2.5

Table 4-73 (Cont.) Policy 23.1.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
34747615	PCF DBTIER GR Broken with Error Code 1022 (duplicate key in table 'NDB$BLOB_1436_7" on query)	The PCF cnDBTier georedundency is broken with Error Code 1022.	This could result in replication link failure if 1022 is not added to skip_slave_error/ replica_slave error list. **Workaround**: Add 1022 to skip_slave_error/ replica_slave error list.	3	22.3.0

> **Note:**
>
> The known bugs from 22.4.x have been forward ported to release 23.1.0.

4.3.10 SCP Known Bugs

SCP 23.1.3 Known Bugs

There are no new known bugs in this release. For existing known bugs, see Table 4-74.

SCP 23.1.2 Known Bugs

There are no new known bugs in this release. For existing known bugs, see Table 4-74.

SCP 23.1.1 Known Bugs

There are no new known bugs in this release. For existing known bugs, see Table 4-74.

Table 4-74 SCP 23.1.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
33594355	Wrong ASM Server Header implementation causes ATS testcase failures	An incorrect ASM server header implementation is causing ATS failures.	Due to ASM issue, some ATS testcases are removed. **Workaround**: Comment out ATS testcases failing due to ASM issue.	4	22.1.0

4.3.11 SEPP Known Bugs

SEPP Release 23.1.4 Known Bugs

There are no known bugs in this release.

SEPP Release 23.1.3 Known Bugs

There are no known bugs in this release.

Table 4-75 SEPP Release 23.1.2 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
35488448	n32f-context is taking time to reflect in n32f_db_context table	In some random scenarios, handshake is completed with remote peer. However, the n32f-context entry takes time to reflect in n32f_db_context table. Due to this delay, handshake status curl command shows the context blank even though it is completed.	There will be a delay of five minutes in populating the n32f-context table, but the table will get populated with the correct and latest handshake status resulting in the correct output. **Workaround:** No workaround available	3	23.1.0
35208390	SEPP-Upgrade: cn32f and pn32f pods restart observed during cndb rollback from 23.1.0 to 22.4.0	cn32f and pn32f pods restart observed during cndb rollback from 23.1.0 to 22.4.0	All the cn32f and pn32f pods will get restarted during cnDBTier rollback. The traffic will get impacted, but the system will be self-recovered. **Workaround:** No workaround available	3	23.1.0

Table 4-76 SEPP ATS Release 23.1.2 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
35337221	SEPP ATS installation failed on Tanzu Cluster	SEPP ATS installation failed on Tanzu Cluster during Helm installation. `ocats ocats-sepp-23.1.2.tgz -f ocats_ocsepp_values_23.1.2_ys-sepp_v1.yaml -n ys-sepp` **Error:** unable to build kubernetes objects from release manifest: [unable to recognize "": no matches for kind "ServiceEntry" in version "networking.istio.io/v1alpha3", unable to recognize "": no matches for kind "VirtualService" in version "networking.istio.io/v1alpha3"]	Helm installation of ATS package fails in non-ASM setup and succeeds in the ASM setup. **Workaround:** • Delete the `serviceEntry.yaml` and `virtualService.yaml` from the template. • Perform the Helm install for ATS, and the deployment will be successful. • Add the following file: `createServiceEntryAndvirtualService.yaml`. As an outcome, the same CRD will be created and Helm install will be successful. The following will be created: – `customresourcedefinition.apiextensions.k8s.io/serviceentries.networking.istio.io` is created. – `customresourcedefinition.apiextensions.k8s.io/virtualservices.networking.istio.io` is created.	2	23.1.2

SEPP Release 23.1.1 Known Bugs

There are no new known bugs in this release. For existing known bugs, see Table 4-77.

Table 4-77 SEPP Release 23.1.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
35036599	Total traffic loss after upgrade when global Ingress rate limiting feature is enabled	There is a total traffic failure when SEPP is upgraded from 22.3.x, 224.x to 23.1.0, and rate limit feature is ON. Noticed the below exception after upgrade and also traffic is fine if Ingress pod is restarted. Role=SpringframeworkBootLoaderJarLauncher)) io.github.bucket4j.BucketConfiguration; class invalid for deserialization"," message":"(Wrapped: Failed request execution for MapDistCache service on Member(Id=2)	If global RateLimiting feature is enabled, traffic is in progress and upgrade is performed to 22.4.x or 23.1.0 release, after upgrade n32-ingress-gateway will stop processing traffic. There will be total loss. **Workaround**: Following three workarounds can be used: • If SBI traffic is in progress during upgrade, after upgrade restart the n32-ingress-gateway. System will recover and start processing traffic. • Perform an upgrade with globalRateLimiting feature = disabled	2	22.4.0

Table 4-77 (Cont.) SEPP Release 23.1.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
			• Perform an upgrade to 23.1.0 without traffic.		
34569424	Proper error-reason should be thrown by csepp when n32-ingress service is scaled down at psepp and an interplmn request is sent from csepp to psepp	The scenario is observed when Egress Gateway is not able to send the SBI message to next node or NF, when the NF is unreachable. - HTTP error status in response received by gateway and the details can be configured through values.yaml file - Code exception mentioned in error-reason is coming from EGRESS-GATEWAY code Exception: org.springframework.web.reactive.function.client.WebClientRequestException:nested exception is java.nio.channels.ClosedChannelException	From the error cause, user will not able to identify the reason of failure. They have to check the grafana and metrics to find the root cause. Run kubectl command to verify that all the services are up and running. **Workaround**: Run kubectl command to verify that all the services are up and running. Wait for the service to come up and issue will get resolved.	3	22.2.0

Table 4-77 (Cont.) SEPP Release 23.1.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
34664359	SEPP micro services traces are not correlated in Jaeger UI	In previous versions, when querying traces on Jaeger UI, one single trace was returned with multiple spans from the different microservices involved for a single transaction. Example: plmn-ingress-gateway span + cn32f span + n32-egress-gateway span. In 22.3, this correlation is not occuring and every microservice is generating a different trace.	No functional impact. Correlation was helpful to quickly understand the internal flow of the transaction and find in which particular microservice a potential problem was happening. **Workaround** : Logs on kibana can be used to check correlation of messages.	3	22.3.0

Table 4-77 (Cont.) SEPP Release 23.1.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
34760842	RH SEPP doesn't set a proper authorities in established N32 context with 3GppSbiTargetApiRootSupported" set to false	Remote Host (RH) SEPP attempts to establish N32 context with Remote SEPP1 and Remote SEPP2. Remote SEPP1 - n32c handshake request with "3GppSbiTargetApiRootSupported" set to true in the http body. Remote SEPP2 - n32c handshake request with "3GppSbiTargetApiRootSupported" set to false in the http body. RH SEPP handshake status reflects that THE established N32 context with Remote SEPP2 has 3GPP SBI Target API Root Header Supported set to false The outgoing request from RH SEPP to Remote SEPP2 has no 3gpp-sbi-target-apiroot but the authority is replaced by the remote SEPP2 SEPP identity. This behaviour is incorrect and RH SEPP should set 'authority' header using the value from 3gpp-sbi-target-apiroot header from the incoming request.	When both the consumer and producer SEPPs are Oracle SEPP, the issue will not be observed. Issue will be observed when one of the SEPP is non-Oracle SEPP. **Workaround**: Send a message with 3gpp-sbi-target-api-root header and 3GppSbiTargetApiRootSupported to be set to TRUE in Helm.	3	22.3.0

Table 4-77 (Cont.) SEPP Release 23.1.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
35047654	cnDBTier MIB does not comply estandar RFC2578	When cnDBTier snmp traps are integrated into alarm system, some errors are observed that make the OCDBTIER-MIB.MIB fail in the compilation process and it has to be changed manually. Most common errors: 1. NOTIFICATION-TYPE names that start by uppercase. 2. MIBs must comply with estandar RFC2578.	Alarms system would not get alerts due to CnDBTier related issues. **Workaround**: Manually change the MIB file for the errors observed.	3	22.4.0
34829487	ATS SEPP 22.3.1 unable to deploy stubserver	ATS cases giving "Remote Sepp already present " alert, when remote SEPP is not even present in database. This will make some of the ATS test cases to fail.	Some of the ATS test cases start failing when ATS regression pipeline is running. **Workaround**: Rerun the failed cases manually one by one and they shall pass.	3	22.4.0

Table 4-77 (Cont.) SEPP Release 23.1.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
34374452	SEPP-COM-xx-ERROR-0103 not observed when n32c pods have been scaled down	On scaling down pn32c and cn32c pods, if a delete request is run for the configured remotesepp, error code 204 is returned but entry is not deleted. Also, no error is displayed when POST request is run, when the pods are scaled down.	No impact. Run the delete command when all the pods and services are Up ad running. **Workaround** : Ensure that the the pod and serviceare up. Run the command and it will be executed successfully.	4	22.3.0

4.3.12 UDR Known Bugs

UDR 23.1.3 Known Bugs

There are no new known bugs in this release. For existing known bugs, see Table 4-78.

UDR 23.1.2 Known Bugs

There are no new known bugs in this release. For existing known bugs, see Table 4-78.

UDR 23.1.1 Known Bugs

There are no new known bugs in this release. For existing known bugs, see Table 4-78.

Table 4-78 UDR 23.1.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35041066	Discrepancy in UDR 22.4.1 installation yaml file	There is discrepancy in UDR 22.4.1 installation yaml file on percentage based PDB configuration.	The NRF client supports only percentage based PDB configuration and not decimal values. This is not affecting any functionality. **Workaround**: No workaround available	3	22.4.1
34756798	UDR security vulnerability: readOnlyRootFilesystem Set to False	The readOnlyRootFilesystem in the yaml file is set to False. This controls whether a container is able to write into the root file system.	No impact **Workaround**: Requires changes across multiple services and security impact is low.	3	22.3.0
34940342	EIR PDBI DLT_EIR is not deleting the KEY from EIR DATA if executed immediately after Update	If upd_eir or dlt_eir is executed before ent_eir, the upd_eir or dlt_eir will fail.	No impact **Workaround**: The same set of keys must not be added in source PDBI file.	3	22.4.0

4.3.13 Common Services Known Bugs

4.3.13.1 Alternate Route Service Known Bugs

Release 23.1.0

There are no known bugs in this release.

4.3.13.2 App-Info Known Bugs

Release 23.1.0

There are no known bugs in this release.

4.3.13.3 ASM Configuration Known Bugs

Release 23.1.0

There are no known bugs in this release.

4.3.13.4 ATS Known Bugs

Table 4-79 ATS 23.1.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35081861	Jenkins displays success status even if execution stopped due to behave being killed abruptly.	When the build process was abruptly terminated, Jenkins would sometimes print the build status as a success even though the run was not completed. This should have been reported as an unstable build.	No impact **Workaround**: No workaround available	3	23.1.0
34609837	Jenkins doesn't list test cases when scenario outlines are used	When scenario outlines are used in a feature file, Jenkins is unable to list the test cases when the feature is selected.	No impact **Workaround**: No workaround available	3	22.1.0

4.3.13.5 Debug Tool Known Bugs

Release 23.1.0

There are no known bugs in this release.

4.3.13.6 Egress Gateway Known Bugs

Release 23.1.0

There are no known bugs in this release.

4.3.13.7 Ingress Gateway Known Bugs

Release 23.1.0

There are no known bugs in this release.

4.3.13.8 Helm Test Known Bugs

Release 23.1.0

There are no known bugs in this release.

4.3.13.9 Mediation Known Bugs

Release 23.1.0

There are no known bugs in this release.

4.3.13.10 NRF-Client Known Bugs

Release 23.1.0

There are no known bugs in this release.

4.3.13.11 Perf-Info Known Bugs

Release 23.1.0

There are no known bugs in this release.