Oracle® Communications

Cloud Native Core Release Notes

Release 2.23.3
F85945-21
September 2024

Oracle Communications Cloud Native Core Release Notes, Release 2.23.3

F85945-21

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 2.23.3 - F85945-21, September 2024

CNE 23.3.5 Release

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

Release 2.23.3 - F85945-20, May 2024

cnDBTier 23.3.3 Release

Updated the known bugs for 23.3.3 in the cnDBTier Known Bugs section.

Release 2.23.3 - F85945-19, May 2024

CNE 23.3.5 Release

Updated the following sections with the details of CNE release 23.3.5:

- Media Pack
- Compatibility Matrix
- CNE Resolved Bugs

Release 2.23.3 - F85945-18, April 2024

cnDBTier 23.3.3 Release

Updated the following sections with the details of cnDBTier release 23.3.3:

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

Release 2.23.3 - F85945-16, April 2024

NRF 23.3.0 Release

Added 36137134 bug in the NRF Known Bugs section.

Release 2.23.3 - F85945-15, February 2024

NEF 23.3.2 Release

Updated the following sections with the details of NEF release 23.3.2:

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

SEPP 23.3.2 Release

Updated the following sections with the details of SEPP release 23.3.2:

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

UDR 23.3.2 Release

Updated the following sections with the details of UDR release 23.3.2:

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

Release 2.23.3 - F85945-14, January 2024

CNC Console 23.3.2 Release

Updated the following sections with details of CNC Console release 23.3.2:

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

NRF 23.3.2 Release

Updated the following sections with the details of NRF release 23.3.2:

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

SCP 23.3.2 Release

Updated the following sections with the details of SCP release 23.3.2:

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

Release 2.23.3 - F85945-13, January 2024

cnDBTier 23.3.2 Release

Updated the following sections with the details of cnDBTier release 23.3.2:

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

CNE 23.3.4 Release

Updated the following sections with the details of CNE release 23.3.4:

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

Release 2.23.3 - F85945-12, January 2024

NRF 23.3.1 Release

Made formatting changes.

Release 2.23.3 - F85945-11, December 2023

SCP 23.3.1 Release

Added a new bug 36089521 in the SCP Resolved Bugs section.

Release 2.23.3 - F85945-10, December 2023

NSSF 23.3.1 Release

Updated the following section with supported Kubernetes version for NSSF:

- Compatibility Matrix

Release 2.23.3 - F85945-09, November 2023

CNE 23.3.3 Release

Updated the following sections with the details of CNE release 23.3.3:

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

CDCS 23.3.1 Release

Updated the following sections with the details of CDCS release 23.3.1:

- Continuous Delivery Control Server (CDCS)
- Media Pack

- Compatibility Matrix
- CDCS Resolved Bugs
- CDCS Known Bugs

Release 2.23.3 - F85945-08, October 2023

cnDBTier 23.3.1 Release

Updated the following sections with the details of cnDBTier release 23.3.1:

- Media Pack
- Compatibility Matrix
- cnDBTier Resolved Bugs

NEF 23.3.1 Release

Updated the following sections with the details of NEF release 23.3.1:

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

NRF 23.3.1 Release

Updated the following sections with the details of NRF release 23.3.1:

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

NSSF 23.3.1 Release

Updated the following sections with the details of NSSF release 23.3.1:

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

SCP 23.3.1 Release

Updated the following sections with the details of SCP release 23.3.1:

- Service Communication Proxy (SCP)
- Media Pack
- Compatibility Matrix

- Common Microservices Load Lineup
- Security Certification Declaration
- SCP Resolved Bugs
- SCP Known Bugs

SEPP 23.3.1 Release

Updated the following sections with the details of SEPP release 23.3.1:

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

UDR 23.3.1 Release

Updated the following sections with the details of UDR release 23.3.1:

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

CNE 23.3.2 Release

Updated the following sections with the details of CNE release 23.3.2:

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

Release 2.23.3 - F85945-07, October 2023

CNC Console 23.3.1 Release

Updated the following sections with the details of CNC Console release 23.3.1:

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

Release 2.23.3 - F85945-06, October 2023

SCP 23.3.0 Release

Updated the section reference in the Service Communication Proxy (SCP) section.

Release 2.23.3 - F85945-05, October 2023

cnDBTier 23.3.0 Release

Added a bug in the cnDBTier Known Bugs section.

Release 2.23.3 - F85945-04, September 2023

CD Control Server 23.3.0 Release

Updated the following sections with the details of CDCS release 23.3.0:

- Continuous Delivery Control Server (CDCS)
- Media Pack
- Compatibility Matrix
- 3GPP Compatibility Matrix
- CDCS Resolved Bugs
- CDCS Known Bugs

CNC Console 23.3.0 Release

Updated the Cloud Native Configuration Console (CNC Console) section.

Release 2.23.3 - F85945-03, September 2023

CNE 23.3.1 Release

Updated the following sections with the details of CNE release 23.3.1:

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

Release 2.23.3 - F85945-02, September 2023

CNC Console 23.3.0 Release

Updated the following sections with the details of CNC Console release 23.3.0:

- Cloud Native Configuration Console (CNC Console)
- Media Pack
- Compatibility Matrix
- 3GPP Compatibility Matrix
- Common Microservices Load Lineup
- Security Certification Declaration

- CNC Console Resolved Bugs

NEF 23.3.0 Release

Updated the following sections with the details of NEF release 23.3.0:

- Network Exposure Function (NEF)
- Media Pack
- Compatibility Matrix
- 3GPP Compatibility Matrix
- Common Microservices Load Lineup
- Security Certification Declaration
- NEF Resolved Bugs
- NEF Known Bugs

NRF 23.3.0 Release

Updated the following sections with the details of NRF release 23.3.0:

- Network Repository Function (NRF)
- Media Pack
- Compatibility Matrix
- 3GPP Compatibility Matrix
- Common Microservices Load Lineup
- Security Certification Declaration
- NRF Resolved Bugs
- NRF Known Bugs

NSSF 23.3.0 Release

Updated the following sections with the details of NSSF release 23.3.0:

- Network Slice Selection Function (NSSF)
- Media Pack
- Compatibility Matrix
- 3GPP Compatibility Matrix
- Common Microservices Load Lineup
- Security Certification Declaration
- NSSF Resolved Bugs
- NSSF Known Bugs

SCP 23.3.0 Release

Updated the following sections with the details of SCP release 23.3.0:

- Service Communication Proxy (SCP)
- Media Pack
- Compatibility Matrix
- 3GPP Compatibility Matrix

- Common Microservices Load Lineup
- Security Certification Declaration
- SCP Resolved Bugs
- SCP Known Bugs

SEPP 23.3.0 Release

Updated the following sections with the details of SEPP release 23.3.0:

- Security Edge Protection Proxy (SEPP)
- Media Pack
- Compatibility Matrix
- 3GPP Compatibility Matrix
- Common Microservices Load Lineup
- Security Certification Declaration
- SEPP Resolved Bugs
- SEPP Known Bugs

UDR 23.3.0 Release

Updated the following sections with the details of UDR release 23.3.0:

- Unified Data Repository (UDR)
- Media Pack
- Compatibility Matrix
- 3GPP Compatibility Matrix
- Common Microservices Load Lineup
- Security Certification Declaration
- UDR Resolved Bugs
- UDR Known Bugs

Common Services Resolved Bugs

Updated the following sections with the details of Common Services Resolved Bugs for Release 23.3.x:

- Egress Gateway Resolved Bugs
- Ingress Gateway Resolved Bugs
- NRF-Client Resolved Bugs
- ATS Resolved Bugs

Common Services Known Bugs

Updated the following sections with the details of Common Services Known Bugs for Release 23.3.x:

- Egress Gateway Known Bugs

Release 2.23.3 - F85945-01, August 2023

cnDBTier 23.3.0 Release

Updated the following sections with the details of cnDBTier release 23.3.0:

- Cloud Native Core cnDBTier
- Media Pack
- Compatibility Matrix
- cnDBTier Resolved 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 2.23.3.

2.1 Continuous Delivery Control Server (CDCS)

Release 23.3.1

The following enhancements are made in release 23.3.1.

- **Support for updating Oracle Linux**: CDCS allows to update the base Oracle Linux version for CDCS VMs and the host OS (when CDCS is installed on a BareMetal server) with the latest version. For more information about the Oracle Linux version, see the *Oracle Communications CD Control Server Installation and Upgrade Guide*.
- **Support for CNE releases**: CDCS supports the installation and upgrade of CNE releases 22.4.x, 23.1.x, 23.2.x, and 23.3.x. A specific release can be installed by selecting the supported release versions while running the **Install OCCNE** and **Upgrade OCCNE** commands. For more information about selecting the versions, see the "*Managing CNE*" section in *Oracle Communications CD Control Server User Guide*.

Release 23.3.0

Oracle Communications CD Control Server (CDCS) 23.3.0 has been updated with the following enhancements:

- **Support for adding or removing worker nodes at managed sites**: CDCS allows to add or remove worker nodes to CNE at a managed site. This feature is applicable to both production and staging sites, that run on Bare Metal infrastructure only.
  For more information about adding or removing the worker nodes at managed sites, see the "Site Maintenance" section in *Oracle Communications CD Control Server User Guide*.
- **Support for Command Chaining:** This feature enables the user to run multiple commands in a sequence. This feature helps to configure a list of commands to run in a specific order. Enter all the parameter values for the commands in the chain. The commands run sequentially. By default, when the first command completes successfully, the second command runs, and so on. If any command fails, the other commands configured in the chain don't run. (However, the user can select to skip the failed command and proceed with the next command.) A command chain can run immediately or at a specific time.
  For more information about support for command chaining, see the "Command Chaining" section in *Oracle Communications CD Control Server User Guide*.
- **Support for Timeout parameter**: With this enhancement, the user can configure the timeout parameter for certain commands, which takes more than the default time set by CDCS. The TIMEOUT value for any specific lifecycle operation is based on the NF documentation. Otherwise, use the default value of 5 minutes. The following commands have the timeout parameter:
  - Uninstall NF
  - NF Health Check

  - Rollback NF Upgrade
  - Install ATS Tests for NF

  For more information about configuring the TIMEOUT parameter, see the "Managing NF Lifecycle " and "Managing NF Test (staging sites only)" sections in *Oracle Communications CD Control Server User Guide*.

- **Support for new commands**: CDCS supports the following new commands:
  - Delete OCCNE Release
  - Delete ATS Tests for NF Release
  - Uninstall ATS Tests for NF
  - Remove Mate CDCS

  For more information about the new commands, see the sections "Deleting CNE Release", "Deleting ATS Tests for NF Release", "Uninstalling ATS Tests for NF", and "Detaching an Active and Standby CDCS pair" in *Oracle Communications CD Control Server User Guide*.
- **CDCS UI enhancements**: The enhancements in CDCS UI organize the commands in a folder based on operations to ease the use for operators. The main UI screen appears as follows:

Table 2-1 CDCS UI enhancements

Folder	Description
CDCS Configuration	Provides a list of commands used for configuring CDCS.
CDCS Lifecycle	Provides a list of CDCS lifecycle commands.
Production Sites	Provides a list of commands that operate on production sites.
Staging Sites	Provides a list of commands that operate on staging sites.
Site Maintenance	Provides a list of commands that perform maintenance operations at production and staging sites.
NF Lifecycle	Provides a list of NF lifecycle commands.
NF Test	Provides a list of NF ATS test lifecycle commands.
CDCS Internal	Contains the commands that operate on command chains.
Command Chaining	Contains the CDCS internal commands.

For more detailed information about the features released in 23.3.0, see *Oracle Communications CD Control Server User Guide*.

For more detailed information about the features released in CDCS 23.3.x, see *Oracle Communications CD Control Server User Guide*.

2.2 Cloud Native Configuration Console (CNC Console)

Release 23.3.2

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

Release 23.3.1

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

Release 23.3.0

Oracle Communications Cloud Native Configuration Console (CNC Console) 23.3.0 has been updated with the following enhancements:

- **Support for dual stack IPv4 deployment**: Applications or NFs can establish connections with pods and services in a Kubernetes cluster using IPv4 or IPV6 by using the dual stack mechanism. CNC console uses IPv4 by default but can be configured to use either IPv4 or IPv6.
- **Support for IPv6 on IPv6 only infrastructure**: CNC Console can be configured to work on an IPv6 only infrastructure.
- **NF Versions Supported by CNC Console**: The following NF versions are supported in this release:
  - SCP - 23.3.x
  - NRF - 23.3.x
  - UDR - 23.3.x
  - POLICY - 23.2.x
  - BSF - 23.2.x
  - SEPP - 23.3.x
  - NSSF - 23.3.x
  - OCNADD - 23.3.x
  - OCNWDAF - 23.3.x
  - PROVGW - 23.3.x

2.3 Cloud Native Environment (CNE)

> **Note:**
>
> The procedure to update OpenStack credentials is revised in the 23.3.5 User Guide. If you are updating OpenStack credentials on other versions of 23.3.x, refer to the latest procedure from 23.3.5 *Oracle Communications Cloud Native Core, Cloud Native Environment User Guide*.

Release 23.3.5

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

Release 23.3.4

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

Release 23.3.3

Oracle Communications Cloud Native Core, Cloud Native Environment (CNE) 23.3.3 has been updated with the following enhancements:

> **Note:**
>
> The following feature was introduced in 23.3.2 which is an installation-only patch. Therefore, if you are upgrading to 23.3.3 release, be informed about the following feature that is already in place.

- **Fluent Bit replaced with Fluentd OpenSearch**: With release 23.3.2, 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.
  - CNE Environment upgrading from 23.3.1 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 resources requirements of OpenSearch differs according to these metric collection.

Release 23.3.2

Oracle Communications Cloud Native Core, Cloud Native Environment (CNE) 23.3.2 has been updated with the following enhancements:

- **Fluent Bit replaced with Fluentd OpenSearch**: With this release, Fluent Bit is replaced with Fluentd OpenSearch. That is, log forwarding mechanism is changed from fluent-bit to fluentd-openSearch. Additionally, the system creates five OpenSearch data nodes by default.
  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 resources requirements of OpenSearch differs according to these metric collection.
- **New Versions of Common Services**: Fluentd OpenSearch is upgraded to 1.16 in this release.
  To get the complete list of third party services and their versions, refer to the `dependencies_23.3.2.tgz` file provided as part of the software delivery package.

Release 23.3.1

Oracle Communications Cloud Native Core, Cloud Native Environment (CNE) 23.3.1 has been updated with the following enhancements:

- **Secure Container Registry**: CNE uses HTTPS to secure the container registry that runs on Bastion Host. With this implementation, Bastion Host container registry is enabled with TLS and all requests require https connectivity to communicate to the container registry.
- **Grafana Dashboards**: In this release, CNE provisions Grafana dashboards to observe the functioning of CNE components. These dashboards provide metrics about Kubernetes clusters, Opensearch, PVCs, and Prometheus. The dashboards highlight spikes, functional drifts, and performance drifts in the cluster. As Grafana dashboards persist as config maps, users don't have to back up these dashboards during upgrades. For information about this

feature, see *Oracle Communications Cloud Native Core, Cloud Native Environment User Guide*.

- **New Versions of Common Services**: The following common services are upgraded in this release:
  - Helm - 3.12.0
  - Kubernetes - 1.26.5
  - containerd - 1.7.1
  - Calico - 3.26.1
  - MetalLB - 0.13.7
  - Prometheus - 2.44.0
  - Grafana - 9.5.3
  - Jaeger - 1.45.0
  - Istio - 1.18.2
  - Kyverno - 1.9
  - cert-manager - 1.11.0
  - Oracle OpenSearch - 2.3.0
  - Oracle OpenSearch Dashboard - 2.3.0
  - Velero - 1.10

  You can find the complete list of third party services and their versions in the `dependencies_23.3.1.tgz` file provided as part of the software delivery package.
- **Installation and Upgrade Consideration**: In this release, the Bastions mirror UEKR7 along with UEKR6 YUM packages. Therefore, before installing 23.3.x or upgrading to 23.3.x, you must add mirroring of both OL8 UEKR6 and OL8 UEKR7 YUM channels from yum.oracle.com to the central-repository. For more information about configuring YUM repository, see *Oracle Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide*.

Operations Services Overlay (OSO)

Oracle Communications Operations Services Overlay (OSO) 23.3.1 has been updated with the following enhancements:

- **Support for Dualstack**: Using the Dualstack mechanism, applications or NFs can establish connections with pods and services in a Kubernetes cluster using IPv4 or IPv6 or both simultaneously. Dualstack provides:
  - coexistence strategy that allows hosts to reach IPv4 and IPv6 simultaneously.
  - IPv4 and IPv6 allocation to the Kubernetes clusters during cluster creation. This allocation is applicable for all the Kubernetes resources unless explicitly specified during the cluster creation.

  For more information about enabling Dualstack, see "*Installation using CSAR*" and "*Using OSO with IPv6*" sections in *Oracle Communications Operations Services Overlay Installation and Upgrade Guide.*
- **Support for new version of Prometheus**: Prometheus is uplifted from 2.39.1 to 2.44.0.

2.4 Cloud Native Core cnDBTier

Release 23.3.3

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

Release 23.3.2

Oracle Communications Cloud Native Core, cnDBTier (cnDBTier) 23.3.2 has been updated with the following features or feature enhancements:

- **dbtrecover Support for Georeplication Recovery Between Different cnDBTier Versions:** With this feature, the `dbtrecover` script supports georeplication recovery between sites that are running on different cnDBTier versions. For more information about this feature, see the "Recovering Georeplication Sites Using dbtrecover" section in . **Considerations:** Consider the following conditions before using the `dbtrecover` script for performing a georeplication recovery between sites running on different cnDBTier versions:
  - The script supports georeplication recovery between sites only in the following cases:
    - The good site and the bad site (the site to be recovered) run the same cnDBTier version.
    - The good site runs a lower cnDBTier version. However, the cnDBTier release on both the good site and the bad site supports the same database replication REST API.
  - The script doesn't support georeplication recovery between sites in the following cases:
    - The good site runs a cnDBTier version that is higher than the version on the bad site.
    - The good site runs a lower cnDBTier version and uses a different database replication REST API from the one used by the bad site.
  - The following cnDBTier versions use the old database replication API:
    - cnDBTier versions below 22.4.2
    - cnDBTier version 23.1.0
  - The following cnDBTier versions use the new database replication API:
    - cnDBTier versions greater than or equal to 22.4.2 and less than 23.1.0
    - cnDBTier version greater than or equal 23.1.1
- **Support for New Version of Spring Boot**: Spring Boot is upgraded to 3.1.6 in this release.
- **TLS Support for Georeplication**: TLS feature is not supported in this release.

Release 23.3.1

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

Release 23.3.0

Oracle Communications Cloud Native Core, cnDBTier (cnDBTier) 23.3.0 has been updated with the following enhancements:

- **REST APIs to display cnDBTier data on CNC Console**: With this feature, cnDBTier exposes the following REST APIs to CNC Console:
  - Site specific real time replication status
  - Real-time overall replication status
  - Real-time local cluster status
  - cnDBTier version

  These REST APIs will be used by CNC Console in the future releases to fetch cnDBTier data and display them on the CNC Console GUI. This way, cnDBTier facilitates users to integrate cnDBTier on CNC Console and allows users to perform cnDBTier read operations such as checking the status of cnDBTier clusters and georeplication on CNC Console. For more information about the feature and the REST APIs, see *Oracle Communications Cloud Native Core, cnDBTier User Guide*.
- **Secure transfer of backups to remote servers**: With this release, cnDBTier provides the functionality to securely transfer the backups stored in the data nodes to remote sites using Secure File Transfer Protocol (SFTP). This ensures that the database backups are not lost due to purging in cnDBTier as the backups are retained in a remote storage. For more information about enabling and configuring this feature, see *Oracle Communications Cloud Native Core, cnDBTier User Guide* and *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*.
- **Support for new versions of software**: The following software are upgraded in this release:
  - Oracle MySQL Cluster Database - 8.0.34
  - Spring Boot - 3.1.2

2.5 Network Exposure Function (NEF)

Release 23.3.2

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

Release 23.3.1

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

Release 23.3.0

Oracle Communications Cloud Native Core, Network Exposure Function (NEF) 23.3.0 has been updated with the following enhancements:

- **Support for Device Trigger**: This feature enables AFs to send device trigger requests to UEs to perform application-specific tasks such as initiating communication with AF. For more information, see *Oracle Communications Cloud Native Core, Network Exposure Function User Guide* and *Oracle Communications Cloud Native Core, Network Exposure Function Installation, Upgrade, and Fault Recovery Guide*.
- **Support for Converged SCEF-NEF for QoS**: This feature enables converged SCEF-NEF model to set up an AF Session with the required QoS in the 4G system as a fallback solution in case AF session with QoS subscription fails in the 5G system. For more information, see *Oracle Communications Cloud Native Core, Network Exposure Function User Guide* and *Oracle Communications Cloud Native Core, Network Exposure Function Installation, Upgrade, and Fault Recovery Guide*.

2.6 Network Repository Function (NRF)

Release 23.3.2

Supports Service Level Priority with the same Service Names: The Preferred Locality priority handling has been enhanced to support service level priority with same service names. For service-name based discovery query, NRF updates the profile level priority and service level priority of the NF profile if there are multiple services in the NF profile with the same service name after processing the discovery query. For more information about the feature, see *"Preferred Locality"* in *Oracle Communications Cloud Native Core, Network Repository Function User Guide*.

Release 23.3.1

Ingress Gateway Pod Protection: This feature is enhanced to support an additional congestion state parameter, Pending Message Count, for measuring the states. For more information about the feature, see *"Ingress Gateway Pod Protection"* in *Oracle Communications Cloud Native Core, Network Repository Function User Guide*.

Release 23.3.0

Oracle Communications Cloud Native Core, Network Repository Functions (NRF) 23.3.0 has been updated with the following enhancement:

- **Ingress Gateway Pod Protection**: This feature protects the Ingress Gateway pods from getting overloaded due to uneven traffic distribution, traffic bursts, and congestion. It ensures the protection and mitigation of pods from entering an overload condition, while also facilitating necessary actions for recovery. For more information about the feature, see the "*Ingress Gateway Pod Protection*" section in *Oracle Communications Cloud Native Core, Network Repository Function User Guide*.
- **Pre and Post Install/Upgrade Infrastructure Validation**: NRF validation checks are enhanced to support infrastructure validations for preinstallation and preupgrade to verify the NRF version, Kubernetes version, cnDBTier version, replication status, and alerts. For more information about the feature, see the "*Pre and Post Install/Upgrade Validations*" section in *Oracle Communications Cloud Native Core, Network Repository Function User Guide*.
- **Dynamic SLF Selection based on Extended Preferred Locality Feature Configuration**: When Extended Preferred Locality feature is enabled, the sorting and prioritizing of the SLF or UDR profiles for SLF selection is performed based on the feature configuration. For more information about the feature, see the "*Subscriber Location Function*" section in *Oracle Communications Cloud Native Core, Network Repository Function User Guide*.
- **Dynamic SLF Selection based on Empty List Feature Configuration**: When Empty List is enabled, the sorting and prioritizing of the SLF or UDR profiles for SLF selection is performed based on the feature configuration. For more information about the feature, see the "*Subscriber Location Function*" section in *Oracle Communications Cloud Native Core, Network Repository Function User Guide*.
- **NRF Deployment using CDCS**: In addition to NRF's Command Line Interface (CLI) deployment method, NRF can be deployed using Continuous Delivery Control Server (CDCS), which is a centralized server that automates NRF deployment processes such as downloading the NRF package, installation, upgrade, and rollback. For more information about CDCS, see Oracle Communications CD Control Server User Guide. For information about NRF deployment using CDCS, see *Oracle Communications Cloud Native Core, Network Repository Function Installation, Upgrade, and Fault Recovery Guide*.

- **Limiting the number of producers based on NF Set Ids**: This feature allows NRF to limit the number of matching NF profiles from the first matching location(s) and other matching locations using the NF Set Ids. For more information about the feature, see "*Preferred Locality Feature Set*" in *Oracle Communications Cloud Native Core, Network Repository Function User Guide*.

2.7 Network Slice Selection Function (NSSF)

Release 23.3.1

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

Release 23.3.0

Oracle Communications Cloud Native Core, Network Slice Selection Function (NSSF) 23.3.0 has been updated with the following enhancements:

- **Support for User-Agent Header**: This feature enables the usage of the User-Agent Header in every HTTP/2 request that NSSF sends over any Service-Based Interface (SBI) to a producer NF such as AMF or NRF. For more information, see "*Support for User-Agent Header in NSSF*" section in *Oracle Communications Cloud Native Core, Network Slice Selection Function User Guide*.
- **Ingress Gateway Pod Protection**: This feature protects the Ingress Gateway pods from getting overloaded due to uneven traffic distribution, traffic bursts, or congestion. It ensures the protection and mitigation of pods from entering an overload condition, while also facilitating necessary actions for recovery. For more information, see "*Ingress Gateway Pod Protection for NSSF*" section in *Oracle Communications Cloud Native Core, Network Slice Selection Function User Guide*.

2.8 Service Communication Proxy (SCP)

Release 23.3.2
No new features or feature enhancements have been introduced in this release.

Release 23.3.1

Oracle Communications Cloud Native Core, Service Communication Proxy (SCP) 23.3.1 has been updated with the following enhancements:

- **Support for 620K MPS with Model C**: Model C is tested with traffic at a rate of 620K MPS. For more information about this testcase scenario, see *Oracle Communications Cloud Native Core, Service Communication Proxy Benchmarking Guide*.

Release 23.3.0

Oracle Communications Cloud Native Core, Service Communication Proxy (SCP) 23.3.0 has been updated with the following enhancements:

- **Routing options enhancement to control SCP routing features**: SCP allows the user to control the applicability of routing features by providing options to enable or disable rerouting at the NF service level. For more information, see "*Routing Options Enhancement to Control SCP Routing Features*" in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.
- **TLS certificate configuration enhancement**: This enhancement enables SCP to configure different Transport Layer Security (TLS) certificates on ingress and egress interfaces. It also allows the user to provide primary and secondary certificates for each

interface. For more information, see "*TLS Certificate Configuration Enhancement*" in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.

- **Support for OCCNE egress NAT**: SCP supports egress NAT in Oracle Communications Cloud Native Core, Cloud Native Environment (CNE). For more information, see "*Configuring Egress NAT for an NF*" in *Oracle Communications Cloud Native Core, Cloud Native Environment User Guide*.

2.9 Security Edge Protection Proxy (SEPP)

Release 23.3.2

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

Release 23.3.1

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

Release 23.3.0

Oracle Communications Cloud Native Core, Security Edge Protection Proxy (SEPP) 23.3.0 has been updated with the following enhancements:

- **Alternate Routing based on the DNS SRV Record for Home Network Functions**: This feature performs alternate routing of messages by querying SRV records with the DNS server to find an alternate producer NF and route the service request. SEPP supports retrieval of NRF, SCP, and Producer NFs' records using DNS SRV queries at plmn-egress-gateway. SEPP uses either NF Set or DNS SRV records to perform alternate routing. For more information about the feature, see the "*Alternate Routing based on the DNS SRV Record for Home Network Functions*" section in *Oracle Communications Cloud Native Core, Security Edge Protection Proxy User Guide* and the "*Configuration Parameters*" section in *Oracle Communications Cloud Native Core, Security Edge Protection Proxy Installation, Upgrade, and Fault Recovery Guide*.
- **Rate Limiting for Egress Roaming Signaling per PLMN**: This feature configures the egress request rate on N32F interface based on the destination PLMN IDs. This controls the messages sent out from the local SEPP to a Remote SEPP. With this feature, the number of egress requests to one or more PLMN IDs is restricted based on a configured count using token bucket algorithm.
  For more information about the feature, see the "*Rate Limiting for Egress Roaming Signaling per PLMN*" section in *Oracle Communications Cloud Native Core, Security Edge Protection Proxy User Guide*, "*Egress Rate Limiting Option Configuration*" section in *Oracle Communications Cloud Native Core, Security Edge Protection Proxy REST API Specification Guide*, and the "*Configuration Parameters*" section in *Oracle Communications Cloud Native Core, Security Edge Protection Proxy Installation, Upgrade, and Fault Recovery Guide*.
- **Cat-0 SBI Message Schema Validation Feature Enhancement**: Cat-0 SBI Message Schema Validation Feature Enhancement: The Cat-0 SBI message schema validation feature now supports the SBI header validation. This feature supports stateless security counter measures, which enhances roaming partners to handle the security. For example, only valid requests are allowed to be processed at SEPP at lower layer.
  For more information about the feature, see the "*Cat-0 SBI Message Schema Validation Feature*" section in *Oracle Communications Cloud Native Core, Security Edge Protection Proxy User Guide*.

2.10 Unified Data Repository (UDR)

Release 23.3.2

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

Release 23.3.1

Oracle Communications Cloud Native Core, Unified Data Repository (UDR) 23.3.1 has been updated with the following enhancements:

- **Error Response Enhancement for SLF Lookup Request**: The error response is enhanced to support error causes scenario for SLF lookup requests. SLF supports the "cause" attribute in the problem details for all error responses as per 3GPP 29.504 specification. The "cause" attribute in the problem details object of the HTTP error response payload is used to indicate the application-related information for that specific error occurrence. This enables the HTTP client to take appropriate action. For more information about the feature, see "*Error Response Enhancement for SLF Lookup Request*" section in *Oracle Communications Cloud Native Core, Unified Data Repository User Guide.*

Release 23.3.0

Oracle Communications Cloud Native Core, Unified Data Repository (UDR) 23.3.0 has been updated with the following enhancements:

- **Converged Quota Support for UDR**: Converged Quota Support for UDR updates the data model to support storage of 4G policy quota and dynamic quota under sm-data/umData and sm-data/umDataLimits respectively from VSA. On-demand migration and Diameter-sh are enhanced to support converged quota. For more information about the feature, see "*Converged Quota Support for UDR*" section in *Oracle Communications Cloud Native Core, Unified Data Repository User Guide*.
- **NF Scoring for a Site Integration with CNC Console**: UDR supports the Network Function (NF) Scoring feature to calculate the site score based on NF specific factors such as alerts. The NF Scoring feature helps the operator to determine the health of a site. In this release, the NF Scoring feature can be configured using CNC Console. For more information about the feature, see "*NF Scoring for a Site*" and "*NF Scoring Configurations*" sections in *Oracle Communications Cloud Native Core, Unified Data Repository User Guide*.
- **Diameter Connection Configuration**: The Diameter Connection Configuration triggers a Connection Establishment Request (CER) from the Diameter Gateway pod to each of the configured diameter endpoints. This feature enables the distribution of the diameter connection in a controlled manner by balancing the diameter traffic evenly between the Diameter Gateway pods. This is achieved by adding peer node details as a configuration in the Diameter Gateway. For more information about the feature, see "*Diameter Connection Configuration*" section in *Oracle Communications Cloud Native Core, Unified Data Repository User Guide*.
- **Network Policies**: Network Policies are an application-centric construct that allows you to specify how a pod is allowed to communicate with various network entities. Network Policies create pod-level rules to control communication between the cluster's pods and services. It determines which pods and services can access one another inside the cluster. For more information about the feature, see "*Network Policies*" section in *Oracle Communications Cloud Native Core, Unified Data Repository User Guide* and "*Configuring Network Policies*" section in *Oracle Communications Cloud Native Core, Unified Data Repository Installation, Upgrade, and Fault Recovery Guide*.

- **Conflict Resolution**: In a multisite deployment, UDR updates subscriber data on all the sites during replication down time. When the replication is restored and if there are any conflicts in the subscriber data updates, they are automatically resolved in all the database tables by MySQL NDB Cluster in cnDBTier. However, in some cases, automatic resolution by MySQL causes subscriber data conflicts and anomalies in the database model. This feature provides an application-defined resolution to resolve the subscriber data conflicts by adding a timestamp column to determine whether an update is required on the replica. For more information about the feature, see "*Conflict Resolution*" and 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 2.23.3. 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 2.23.3

Description	NF Version	ATS Version	Upgrade Supported
Oracle Communications CD Control Server (CDCS)	23.3.1	NA	CDCS 23.3.1 supports fresh installation and upgrade from 23.2.x and 23.3.0. For more information, see *Oracle Communications CD Control Server Installation and Upgrade Guide*.
Oracle Communications CD Control Server (CDCS)	23.3.0	NA	CDCS 23.3.0 supports fresh installation and upgrade from 23.2.x. For more information, see *Oracle Communications CD Control Server Installation and Upgrade Guide*.
Oracle Communications Cloud Native Configuration Console (CNC Console)	23.3.2	NA	CNC Console 23.3.2 supports fresh installation and upgrade from 23.1.x, 23.2.x, and 23.3.x. For more information, see *Oracle Communications Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide.*
Oracle Communications Cloud Native Configuration Console (CNC Console)	23.3.1	NA	CNC Console 23.3.1 supports fresh installation and upgrade from 23.1.x, 23.2.x, and 23.3.0. 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 2.23.3

Description	NF Version	ATS Version	Upgrade Supported
Oracle Communications Cloud Native Configuration Console (CNC Console)	23.3.0	NA	CNC Console 23.3.0 supports fresh installation and upgrade from 23.1.x and 23.2.x. 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)	23.3.5	NA	CNE 23.3.5 supports fresh installation and upgrade from 23.2.x and 23.3.x. 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)	23.3.4	NA	CNE 23.3.4 supports fresh installation and upgrade from 23.2.x and 23.3.x. 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)	23.3.3	NA	CNE 23.3.3 supports fresh installation and upgrade from 23.2.x and 23.3.x. 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)	23.3.2	NA	CNE 23.3.2 supports only fresh installation. 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)	23.3.1	NA	CNE 23.3.1 supports fresh installation and upgrade from 23.2.x. For more information, see *Oracle Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Operations Services Overlay (OSO)	23.3.1	NA	OSO 23.3.1 supports fresh installation and upgrade from 23.2.x. For more information, see *Oracle Communications Operations Services Overlay Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core, cnDBTier	23.3.3	NA	cnDBTier 23.3.3 supports fresh installation and upgrade from 23.1.x, 23.2.x, and 23.3.x. 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 2.23.3

Description	NF Version	ATS Version	Upgrade Supported
Oracle Communications Cloud Native Core, cnDBTier	23.3.2	NA	cnDBTier 23.3.2 supports fresh installation and upgrade from 23.1.x, 23.2.x, and 23.3.x. For more information, see *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, cnDBTier	23.3.1	NA	cnDBTier 23.3.1 supports fresh installation and upgrade from 23.1.x, 23.2.x, and 23.3.0. For more information, see *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, cnDBTier	23.3.0	NA	cnDBTier 23.3.0 supports fresh installation and upgrade from 23.1.x and 23.2.x. For more information, see *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Network Exposure Function (NEF)	23.3.2	23.3.2	NEF 23.3.2 supports fresh installation and upgrade from 23.1.x, 23.2.x, and 23.3.x to 23.3.2. 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)	23.3.1	23.3.1	NEF 23.3.1 supports fresh installation and upgrade from 23.1.x, 23.2.x, and 23.3.0. For more information, see *Oracle Communications Cloud Native Core, Network Exposure Function Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Network Exposure Function (NEF)	23.3.0	23.3.0	NEF 23.3.0 supports fresh installation and upgrade from 23.1.x and 23.2.x. 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)	23.3.2	23.3.2	NRF 23.3.2 supports fresh installation and upgrade from 23.2.x and 23.3.x. 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 2.23.3

Description	NF Version	ATS Version	Upgrade Supported
Oracle Communications Cloud Native Core, Network Repository Function (NRF)	23.3.1	23.3.1	NRF 23.3.1 supports fresh installation and upgrade from 23.2.x and 23.3.0. For more information, see *Oracle Communications Cloud Native Core, Network Repository Function Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Network Repository Function (NRF)	23.3.0	23.3.0	NRF 23.3.0 supports fresh installation and upgrade from 23.2.x. 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)	23.3.1	23.3.1	NSSF 23.3.1 supports fresh installation and upgrade from 23.2.x and 23.3.0. 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)	23.3.0	23.3.0	NSSF 23.3.0 supports fresh installation and upgrade from 23.2.x. For more information, see Oracle Communications Cloud Native Core, Network Slice Selection Function Installation, Upgrade, and Fault Recovery Guide.
Oracle Communications Cloud Native Core, Service Communications Proxy (SCP)	23.3.2	23.3.2	SCP 23.3.2 supports fresh installation and upgrade from 23.1.x, 23.2.x, and 23.3.x. 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)	23.3.1	23.3.1	SCP 23.3.1 supports fresh installation and upgrade from 23.1.x, 23.2.x, and 23.3.0. 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)	23.3.0	23.3.0	SCP 23.3.0 supports fresh installation and upgrade from 23.1.x and 23.2.x. 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 2.23.3

Description	NF Version	ATS Version	Upgrade Supported
Oracle Communications Cloud Native Core, Security Edge Protection Proxy (SEPP)	23.3.2	23.3.2	SEPP 23.3.2 supports fresh installation and upgrade from 23.1.x, 23.2.x, and 23.3.x. 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)	23.3.1	23.3.1	SEPP 23.3.1 supports fresh installation and upgrade from 23.1.x, 23.2.x, and 23.3.0. For more information, see *Oracle Communications Cloud Native Core, Security Edge Protection Proxy Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Security Edge Protection Proxy (SEPP)	23.3.0	23.3.0	SEPP 23.3.0 supports fresh installation and upgrade from 23.1.x and 23.2.x. 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)	23.3.2	23.3.2	UDR 23.3.2 supports fresh installation and upgrade from 23.1.x, 23.2.x, and 23.3.x. 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)	23.3.1	23.3.1	UDR 23.3.1 supports fresh installation and upgrade from 23.1.x, 23.2.x, and 23.3.0. 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)	23.3.0	23.3.0	UDR 23.3.0 supports fresh installation and upgrade from 23.1.x and 23.2.x. 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	ASM S/W	Kubernetes	CNC Console	OCNADD
CDCS	23.3.1	• 23.3.x • 23.2.x • 23.1.x • 22.4.x	NA	NA	NA	NA	1.25.x	NA	NA
CDCS	23.3.0	• 23.3.x • 23.2.x • 23.1.x • 22.4.x	NA	NA	NA	NA	1.25.x	NA	NA
CNC Console	23.3.2	• 23.3.x • 23.2.x • 23.1.x	• 23.3.x • 23.2.x • 23.1.x	• 23.3.x • 23.2.x • 23.1.x	• 23.3.x • 23.2.x • 22.3.x	• 1.14.6 • 1.11.8	• 1.26.x • 1.25.x • 1.24.x	NA	23.3.x
CNC Console	23.3.1	• 23.3.x • 23.2.x • 23.1.x	• 23.3.x • 23.2.x • 23.1.x	• 23.3.x • 23.2.x • 23.1.x	• 23.3.x • 23.2.x • 22.3.x	• 1.14.6 • 1.11.8	• 1.26.x • 1.25.x • 1.24.x	NA	23.3.x
CNC Console	23.3.0	• 23.3.x • 23.2.x • 23.1.x	• 23.3.x • 23.2.x • 23.1.x	• 23.3.x • 23.2.x • 23.1.x	• 23.3.x • 23.2.x • 22.3.x	• 1.14.6 • 1.11.8	• 1.26.x • 1.25.x • 1.24.x	NA	23.3.x
CNE	23.3.5	NA	NA	NA	NA	NA	1.26.x	NA	NA
CNE	23.3.4	NA	NA	NA	NA	NA	1.26.x	NA	NA
CNE	23.3.3	NA	NA	NA	NA	NA	1.26.x	NA	NA
CNE	23.3.2	NA	NA	NA	NA	NA	1.26.x	NA	NA
CNE	23.3.1	NA	NA	NA	NA	NA	1.26.x	NA	NA
cnDBTier	23.3.3	• 23.3.x • 23.2.x • 23.1.x	NA	23.2.x	NA	1.11.8	• 1.26.x • 1.25.x • 1.24.x	NA	NA
cnDBTier	23.3.2	• 23.3.x • 23.2.x • 23.1.x	NA	23.2.x	NA	1.11.8	• 1.26.x • 1.25.x • 1.24.x	NA	NA
cnDBTier	23.3.1	• 23.3.x • 23.2.x • 23.1.x	NA	23.2.x	NA	1.11.8	• 1.26.x • 1.25.x • 1.24.x	NA	NA
cnDBTier	23.3.0	• 23.3.x • 23.2.x • 23.1.x	NA	23.2.x	NA	1.11.8	• 1.26.x • 1.25.x • 1.24.x	NA	NA
NEF	23.3.2	• 23.3.x • 23.2.x • 23.1.x	• 23.3.x • 23.2.x • 23.1.x	NA	NA	NA	• 1.26.x • 1.25.x • 1.24.x	NA	NA

Table 3-2 (Cont.) Compatibility Matrix

CNC NF	NF Version	CNE	cnDBTier	CDCS	OSO	ASM S/W	Kubernetes	CNC Console	OCNADD
NEF	23.3.1	• 23.3.x • 23.2.x • 23.1.x	• 23.3.x • 23.2.x • 23.1.x	NA	NA	NA	• 1.26.x • 1.25.x • 1.24.x	NA	NA
NEF	23.3.0	• 23.3.x • 23.2.x • 23.1.x	• 23.3.x • 23.2.x • 23.1.x	NA	NA	NA	• 1.26.x • 1.25.x • 1.24.x	NA	NA
NRF	23.3.2	• 23.3.x • 23.2.x • 23.1.x	• 23.3.x • 23.2.x • 23.1.x	23.3.x	• 23.3.x • 23.2.x • 22.3.x	• 1.14.6 • 1.11.8	• 1.26.x • 1.25.x • 1.24.x	23.3.x	23.3.x
NRF	23.3.1	• 23.3.x • 23.2.x • 23.1.x	• 23.3.x • 23.2.x • 23.1.x	23.3.x	• 23.3.x • 23.2.x • 22.3.x	• 1.14.6 • 1.11.8	• 1.26.x • 1.25.x • 1.24.x	23.3.x	23.3.x
NRF	23.3.0	• 23.3.x • 23.2.x • 23.1.x	• 23.3.x • 23.2.x • 23.1.x	23.3.x	• 23.3.x • 23.2.x • 22.3.x	• 1.14.6 • 1.11.8	• 1.26.x • 1.25.x • 1.24.x	23.3.x	23.3.x
NSSF	23.3.1	• 23.3.x • 23.2.x • 23.1.x	• 23.3.x • 23.2.x • 23.1.x	NA	• 23.3.x • 23.2.x • 22.3.x	• 1.14.6 • 1.11.8	• 1.26.x • 1.25.x • 1.24.x	23.3.x	NA
NSSF	23.3.0	• 23.3.x • 23.2.x • 23.1.x	• 23.3.x • 23.2.x • 23.1.x	NA	• 23.3.x • 23.2.x • 22.3.x	• 1.14.6 • 1.11.8	• 1.26.x • 1.25.x • 1.24.x	23.3.x	NA
SCP	23.3.2	• 23.3.x • 23.2.x • 23.1.x	• 23.3.x • 23.2.x • 23.1.x	• 23.3.x • 23.2.x • 23.1.x	• 23.3.x • 23.2.x • 22.3.x	• 1.14.6 • 1.11.8	• 1.26.x • 1.25.x • 1.24.x	23.3.x	23.3.x
SCP	23.3.1	• 23.3.x • 23.2.x • 23.1.x	• 23.3.x • 23.2.x • 23.1.x	• 23.3.x • 23.2.x • 23.1.x	• 23.3.x • 23.2.x • 22.3.x	• 1.14.6 • 1.11.8	• 1.26.x • 1.25.x • 1.24.x	23.3.x	23.3.x
SCP	23.3.0	• 23.3.x • 23.2.x • 23.1.x	• 23.3.x • 23.2.x • 23.1.x	• 23.3.x • 23.2.x • 23.1.x	• 23.3.x • 23.2.x • 22.3.x	• 1.14.6 • 1.11.8	• 1.26.x • 1.25.x • 1.24.x	23.3.x	23.3.x

Table 3-2 (Cont.) Compatibility Matrix

CNC NF	NF Version	CNE	cnDBTier	CDCS	OSO	ASM S/W	Kubernetes	CNC Console	OCNADD
SEPP	23.3.2	• 23.3.x • 23.2.x • 23.1.x	• 23.3.x • 23.2.x • 23.1.x	• 23.3.x • 23.2.x • 23.1.x	• 23.3.x • 23.2.x • 22.3.x	1.14.6	• 1.26.x • 1.25.x • 1.24.x	23.3.x	23.3.x
SEPP	23.3.1	• 23.3.x • 23.2.x • 23.1.x	• 23.3.x • 23.2.x • 23.1.x	• 23.3.x • 23.2.x • 23.1.x	• 23.3.x • 23.2.x • 22.3.x	1.14.6	• 1.26.x • 1.25.x • 1.24.x	23.3.x	23.3.x
SEPP	23.3.0	• 23.3.x • 23.2.x • 23.1.x	• 23.3.x • 23.2.x • 23.1.x	• 23.3.x • 23.2.x • 23.1.x	• 23.3.x • 23.2.x • 22.3.x	1.14.6	• 1.26.x • 1.25.x • 1.24.x	23.3.x	23.3.x
UDR	23.3.2	• 23.3.x • 23.2.x • 23.1.x	• 23.3.x • 23.2.x • 23.1.x	NA	• 23.3.x • 23.2.x • 22.3.x	• 1.14.6 • 1.11.8	• 1.26.x • 1.25.x • 1.24.x	23.3.x	NA
UDR	23.3.1	• 23.3.x • 23.2.x • 23.1.x	• 23.3.x • 23.2.x • 23.1.x	NA	• 23.3.x • 23.2.x • 22.3.x	• 1.14.6 • 1.11.8	• 1.26.x • 1.25.x • 1.24.x	23.3.x	NA
UDR	23.3.0	• 23.3.x • 23.2.x • 23.1.x	• 23.3.x • 23.2.x • 23.1.x	NA	• 23.3.x • 23.2.x • 22.3.x	• 1.14.6 • 1.11.8	• 1.26.x • 1.25.x • 1.24.x	23.3.x	NA

3.3 3GPP Compatibility Matrix

The following table lists the 3GPP compatibility matrix for each network function:

Table 3-3 3GPP Compatibility Matrix

CNC NF	NF Version	3GPP
CDCS	23.3.x	NA
CNC Console	23.3.x	NA
CNE	23.3.x	NA
cnDBTier	23.3.x	NA

Table 3-3 (Cont.) 3GPP Compatibility Matrix

CNC NF	NF Version	3GPP
NEF	23.3.x	• 3GPP TS 29.122 v16.10.0 • 3GPP TS 23.222 v16.9.0 • 3GPP TS 23.501 v16.10.0 • 3GPP TS 23.502 v16.10.0 • 3GPP TS 29.514 v16.10.0 • 3GPP TS 29.521 v16.10 • 3GPP TS 29.503 v16.14.0 • 3GPP TS 29.515 v16.7 • 3GPP TS 29.222 v16.5.0 • 3GPP TS 29.500 v16.6.0 • 3GPP TS 29.501 v16.6.0 • 3GPP TS 29.522 v16.1 • 3GPP TS 29.510 v16.6.0 • 3GPP TS 29.591 v16.3.0 • 3GPP TS 29.518 v16.14.0 • 3GPP TS 33.501 v17.7.0 • 3GPP TS 29.504 v16.10.0 • 3GPP TS 29.519 v16.11.0 • 3GPP TS 29.508 v16.11.0 • 3GPP TS 23.682 v16.9.0 • 3GPP TS 29.337 v16.1.0 • 3GPP TS 29.214 v16.7.0
NRF	23.3.x	• 3GPP TS 29.510 v15.5 • 3GPP TS 29.510 v16.3.0 • 3GPP TS 29.510 v16.7
NSSF	23.3.x	• 3GPP TS 29.531 v15.5.0 • 3GPP TS 29.531 v16.5.0 • 3GPP TS 29.531 v16.8.0 • 3GPP TS 29.501 v16.10.0 • 3GPP TS 29.502 v16.10.0
SCP	23.3.x	• 3GPP TS 33.310 v16.8.0
SEPP	23.3.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 33.501 v16.5.0 • 3GPP TS 33.117 v16.6.0 • 3GPP TS 33.210 v16.4.0
UDR	23.3.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

> **Note:**
>
> Refer to the Compliance Matrix spreadsheet for details on NFs' compliance with each 3GPP version mentioned in this table.

3.4 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 2.23.3.

Table 3-4 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	23.3.2	NA	NA	NA	NA	NA	23.3.2	NA	23.3.7	23.3.3	NA	NA	NA
CNC Console	23.3.1	NA	NA	NA	NA	NA	23.3.1	NA	23.3.5	23.3.2	NA	NA	NA
CNC Console	23.3.0	NA	NA	NA	NA	NA	23.3.0	NA	23.3.3	23.3.1	NA	NA	NA
NEF	23.3.2	NA	23.3.4	NA	23.3.2	23.3.4	23.3.2	23.3.7	23.3.7	23.3.3	NA	23.3.7	23.3.4
NEF	23.3.1	NA	23.3.2	NA	23.3.1	23.3.2	23.3.1	23.3.5	23.3.5	23.3.2	NA	23.3.5	23.3.2
NEF	23.3.0	NA	23.3.1	NA	23.3.0	23.3.1	23.3.0	23.3.3	23.3.3	23.3.1	NA	23.3.2	23.3.1
NRF	23.3.2	23.3.8	23.3.4	23.3.0	23.3.2	NA	23.3.2	23.3.8	23.3.8	23.3.3	NA	NA	23.3.4
NRF	23.3.1	23.3.6	23.3.2	23.3.0	23.3.1	NA	23.3.1	23.3.6	23.3.6	23.3.2	NA	NA	23.3.2
NRF	23.3.0	23.3.4	23.3.1	23.3.0	23.3.0	NA	23.3.0	23.3.4	23.3.4	23.3.1	NA	NA	23.3.1
NSSF	23.3.1	23.3.5	23.3.2	23.3.0	23.3.0	23.3.2	23.3.1	23.3.5	23.3.5	23.3.2	NA	23.3.5	23.3.2
NSSF	23.3.0	23.3.3	23.3.1	23.3.0	23.3.0	23.3.1	23.3.0	23.3.3	23.3.3	23.3.1	NA	23.3.2	23.3.1
SCP	23.3.2	NA	NA	23.3.0	23.3.2	NA	23.3.2	NA	NA	23.3.3	23.3.2	NA	NA
SCP	23.3.1	NA	NA	23.3.0	23.3.1	NA	23.3.1	NA	NA	23.3.2	23.3.1	NA	NA
SCP	23.3.0	NA	NA	23.3.0	23.3.0	NA	23.3.0	NA	NA	23.3.1	23.3.0	NA	NA
SEPP	23.3.2	23.3.7	23.3.3	23.3.0	23.3.2	23.3.3	23.3.2	23.3.7	23.3.7	23.3.3	23.3.2	23.3.6	23.3.3
SEPP	23.3.1	23.3.5	23.3.2	23.3.0	23.3.2	23.3.2	23.3.1	23.3.5	23.3.5	23.3.2	23.3.1	23.3.5	23.3.2
SEPP	23.3.0	23.3.3	23.3.1	23.3.0	23.3.0	23.3.1	23.3.0	23.3.3	23.3.3	23.3.1	23.3.0	23.3.2	23.3.1
UDR	23.3.2	23.3.7	23.3.4	23.3.0	23.3.2	23.3.4	23.3.2	23.3.7	23.3.7	23.3.3	NA	23.3.7	23.3.4
UDR	23.3.1	23.3.5	23.3.2	23.3.0	23.3.1	23.3.2	23.3.1	23.3.5	23.3.5	23.3.2	NA	23.3.5	23.3.2
UDR	23.3.0	23.3.3	23.3.1	23.3.0	23.3.0	23.3.1	23.3.0	23.3.3	23.3.3	23.3.1	NA	23.3.2	23.3.1

3.5 Security Certification Declaration

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

Table 3-5 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
CNC Console	23.3.2	Jan 29, 2024	Jan 29, 2024	Jan 29, 2024	Aug 25, 2023
CNC Console	23.3.1	Oct 11, 2023	Oct 11, 2023	Oct 11, 2023	Aug 25, 2023
CNC Console	23.3.0	Aug 25, 2023	Aug 25, 2023	Aug 25, 2023	Aug 25, 2023
NEF	23.3.2	Jan 31, 2024	Jan 31, 2024	Jan 31, 2024	Aug 21, 2023
NEF	23.3.1	Oct 13, 2023	Oct 13, 2023	Oct 13, 2023	Aug 21, 2023
NEF	23.3.0	Aug 21, 2023	Aug 21, 2023	Aug 21, 2023	Aug 21, 2023
NRF	23.3.2	Jan 30, 2024	Jan 30, 2024	Jan 30, 2024	Oct 13, 2023
NRF	23.3.1	Oct 13, 2023	Oct 13, 2023	Oct 13, 2023	Oct 13, 2023
NRF	23.3.0	Aug 23, 2023	Aug 23, 2023	Aug 23, 2023	Aug 23, 2023
NSSF	23.3.1	Oct 17, 2023	Oct 17, 2023	Oct 17, 2023	Oct 17, 2023
NSSF	23.3.0	Aug 28, 2023	Aug 28, 2023	Aug 28, 2023	Aug 28, 2023
SCP	23.3.2	Jan 29, 2024	Jan 29, 2024	Jan 29, 2024	Jan 29, 2024
SCP	23.3.1	Oct 13, 2023	Oct 13, 2023	Oct 13, 2023	Oct 13, 2023
SCP	23.3.0	Aug 28, 2023	Aug 28, 2023	Aug 28, 2023	Aug 28, 2023
SEPP	23.3.2	Jan 31, 2024	Jan 31, 2024	Jan 31, 2024	Jan 31, 2024
SEPP	23.3.1	Oct 19, 2023	Oct 19, 2023	Oct 19, 2023	Oct 19, 2023
SEPP	23.3.0	Aug 29, 2023	Aug 29, 2023	Aug 23, 2023	Aug 23, 2023
UDR	23.3.2	NA	Jan 30, 2024	Jan 30, 2024	Jan 30, 2024
UDR	23.3.1	NA	Oct 13, 2023	Oct 13, 2023	Aug 21, 2023
UDR	23.3.0	NA	Aug 21, 2023	Aug 21, 2023	Aug 21, 2023

3.6 Documentation Pack

All documents for Oracle Communications Cloud Native Core (CNC) 2.23.3 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 2.23.3.

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 2.23.3.

4.2.1 CDCS Resolved Bugs

Table 4-1 CDCS 23.3.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35820090	Remove Worker Node pipeline is not waiting for pods to come up.	The Remove OCCNE Worker Node pipeline was failing and it was not waiting until the pods came up.	3	23.3.0

Table 4-2 CDCS 23.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35653383	CNE upgrade is marked as failed as some pods are in terminating status.	CNE upgrade was marked as failed (even when the upgrade script finished successfully), as some pods were in terminated status. When the upgrade script was finished, the following components (pods, nodes, services, and pvcs) were checked to verify if the upgrade process was completed successfully. If some of the pods were on terminating status, then the upgrade process was marked as failure.	3	23.2.0
35574476	CDCS 23.2.0 upgrade failure	CDCS upgrade from 23.1.x to 23.2.0 failed when the `upgrade.sh` was run in the initial phase. It rebooted and the upgrade failed when the `upgrade.sh` command was rerun after the reboot.	3	23.2.0
35547941	CNE upgrade continues even when failing on stage 1	CNE upgrade continued even when an exception was thrown during stage 1 of the upgrade procedure. The process continued and it did not stop until it reached stage 2.	3	23.2.0

Table 4-2 (Cont.) CDCS 23.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35820118	Pipelines are not waiting for helm commands to complete	All Helm commands required a `--wait` flag to be added so that the API calls were blocked until the command was completed. CDCS did not always do this to report a successful command status when the command actually failed.	3	23.2.0
35820143	Missing STAGING on the post-cleanup procedure for Install ATS pipeline	The Install ATS command worked as expected until the procedure reached the post-cleanup phase. It failed and showed the output as "*FAILURE*" in the end.	3	23.2.0

4.2.2 CNC Console Resolved Bugs

Table 4-3 CNC Console 23.3.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35808170	DB Replication break after cncc upgrade from 23.2.0 to 23.3.0	Database Replication broke when CNC Console was upgraded from 23.2.0 to 23.3.0.	2	23.2.0
35938184	Performing a helm upgrade to 23.2 on CNCC causes database replication errors	Performing a Helm upgrade to 23.3.0 in CNC Console caused database replication errors.	2	23.2.0
35974624	CNCC Upgrade to 23.2.1 id failing (part of PCF 23.2.4 Upgrade)	CNC Console upgrade to 23.2.1 failed.	3	23.2.1
35207194	Observing JDBC exception after CNCC Deployment in cm-service	A JDBC exception was seen when CNC Console was deployed in cm-service.	3	23.1.0
35951110	LDAP connection with FQDN not working. Works with IPv6.	LDAP connectivity to the customer's Active Directory server using the IPv6 address was working, however, the LDAP connection with FQDN was not working.	3	23.2.1
36037941	Single Database Restore for CNCC failing	Single Database Restore for CNC Console failed.	3	23.2.0

Table 4-3 (Cont.) CNC Console 23.3.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35999652	CNCC security content and pod security policy	CNC Console security content and pod security policy details were missing from the *Oracle Communications Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide*.	3	23.1.0

CNC Console 23.3.1

There are no resolved bugs in this release.

Table 4-4 CNC Console 23.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35645264	CNCC Deployment Fails in AWS Cluster Running Kubernetes 1.25	When CNC Console was deployed in AWS cluster running Kubernetes 1.25, the deployment failed and the error "no matches for kind "PodDisruptionBudget" in version "policy/vbeta1" was seen. This error was encountered because the Kubernetes version did not follow the standard Major.Minor.Patch versioning and had extra string characters. The CNC Console chart was updated to resolve this issue.	3	23.2.0
35738252	Helm Upgrade to CNC Console v23.2.0 fails with PodDisruptionBudget version mismatch error.	CNC Console Helm upgrade to 23.2.0 failed because of a PodDisruptionBudget version mismatch error. Changes were made to the CNC Console helm chart to resolve this issue.	3	23.2.0

> **Note:**
>
> Resolved bugs from 23.1.2 have been forward ported to Release 23.3.0.

4.2.3 CNE Resolved Bugs

Table 4-5 CNE 23.3.5 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36068408	Grafana issues seen in 23.4	Many panels in Grafana dashboards did not work as the metric expressions used for those channels were deprecated or updated.	3	23.3.4 23.4.0
36465203	Opensearch policy not working - Skylynx2	Opensearch "`hot_Warm_delete`" policy did not work and did not delete the indices.	3	23.4.0
36085028	Issues observed in Opensearch/Fluentd manually uplifted cluster with CNE 23.2.5/2.0	ISM policy had issues with the retention period set for purging indices which impacted the cluster state.	2	23.2.0
36471284	Stage2 of OCCNE Upgrade from 23.2.5 to 23.3.3 failing	During a switchover, the recreate port logic failed in 23.3.x, 23.4.x, and 24.1.x.	2	23.3.3

Table 4-6 CNE 23.3.4 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35369547	Target index not getting deleted as part of ILM	When a targeted index was deleted, it got recreated automatically. This created an issue as the user had to continuously monitor the indexes and manually manage the indexes on CNE. The steps to manage indexes were not functioning as expected.	2	23.1.1
35882687	Opensearch GUI went into the inaccessible state while running traffic at a rate of 10K errors per second from SCP	OpenSearch GUI went into an inaccessible state and displayed the "Opensearch Dashboard server is not ready yet" error while running the traffic from SCP at the rate of 10K error.	2	23.1.0

Table 4-6 (Cont.) CNE 23.3.4 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35527486	SPAD_POLICY: rook-ceph pods are getting restarted	Three Custom Resource Definitions (CRDs) found in `k8s_install/upgrade_/templates/` had `v1beta1` version and didn't get created. As a result, the `csi-snapshotter` container of the `csi-cephfsplugin-provisioner` pod encountered errors while taking snapshots.	2	22.4.3
35882687	Opensearch GUI went into the inaccessible state while running traffic at a rate of 10K errors per second from SCP	OpenSearch data nodes threw HTTP 429 error code when data ingestion rate was very high.	2	23.1.0
36139899	Alertmanager is not able to reach snmp notifier	After an upgrade, the SNMP notifier service was migrated from `occne-snmp-notifier` to `occne-alertmanager-snmp-notifier`, however the alertmanager configuration did not reflect this change.	3	23.2.5

Table 4-7 CNE 23.3.3 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35943796	CNE Upgrade failed while upgrading from 23.3.1 to 23.3.2	CNE upgrade from 23.3.1 to 23.3.2 failed due to multiple reasons.	3	23.3.2
35939310	Steps to add worker node on Bare Metal using addBmWorkerNode.py not work	The `addBmWorkerNode.py` script to add worker node on Bare Metal didn't work. The procedure to add a worker node using `addBmWorkerNode.py` is updated in the CNE user guide from release 23.2.0 onwards.	3	23.3.1

CNE 23.3.2 Resolved Bugs

There are no resolved bugs in this release.

Table 4-8 CNE 23.3.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35147305	Common service pipeline script removing haproxy.cf before removing LB svc in occne-infra	While running the pipeline script to delete the common services deployment, the HAProxy process and `cfg` files were removed before the LB type services in the cluster were deleted. As a result, the interfaces continued to remain attached to the active LBVM. When a redeployment was attempted, the HAProxy files did not get updated as the LB controller pod was getting the 409 HTTP Response from OpenStack.	2	22.4.1
35703638	23.1 to 23.2 CNE upgrade Stage-2 failures when validating LBVMs	During the health status checks, `lb-controller` and `egress-controller` pods continuously got into the `Crashloopbackoff` state and most of the LBVMs failed.	2	23.2.0
35396670	Bastion failover not updating occne-repo-hosts due to "allocation failed; exceeded num_locks (2048)	The `occne_all.sh` script uses the provision container to run commands for all cluster nodes. This script was missing the `` `--rm` `` flag that is used to remove the containers after completion. As a result, every call to the script left an orphaned terminated container in the container space and consumed locks and other resources.	3	22.4.1 22.4.2 22.4.3 23.1.0 23.1.1
35047760	CNE MIB does not comply estandar RFC2578	The objects defined in MIB file are supposed to be displayed in the traps sent through AlertManger and snmp notifier. However, the objects were not displayed in the traps.	3	22.4.0 23.1.0 23.2.0

Table 4-8 (Cont.) CNE 23.3.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35173527	SCP-A is not getting traffic from load balancer	The auto recovery code for LB controller dual failure failed to recover multiple pool LBVMs at once. When all LBVMs failed in multiple pools and came up online at the same time, the LB controller was unable to recover one or more LBVMs and the LBVMs were left in the incomplete state for switchover.	3	22.3.0 22.3.1 22.3.2 22.4.0 22.4.1 23.1.0

Note:

Resolved bugs from 22.4.3, 23.1.2, and 23.2.1 have been forward ported to Release 23.3.1.

OSO 23.3.1

There are no resolved bugs in this release.

4.2.4 cnDBTier Resolved Bugs

Table 4-9 cnDBTier 23.3.3 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36168800	Duplicate channel_id being set for channels in 3 site 6 channel setup leading to replication break	Duplicate channel ID (channel_id) set for channels in a three-site six channel setup resulted in replication halt during a switchover.	2	23.4.0
36229967	cnDBTier alert rules file is incorrect for 23.4.0 release	cnDBTier alert rules file was incorrect for release 23.4.0 and had to be updated.	2	23.4.0
35789744	Unable to run recovery on a 4 site multi channel setup using dbtrecover script	The `dbtrecover` script failed to determine if HTTPS and database encrypt features are enabled in ASM clusters.	2	23.3.0

Table 4-9 (Cont.) cnDBTier 23.3.3 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36271935	Unable to do recovery with DBTRecover as wrong IP is being read in DBTRecover.	The `dbtrecover` script used old IPs to restart `db-replication-svc` pods resulting in recovery failure.	2	23.4.0
36339825	Export variables used from OCCNE	Users used `OCCNE_NAMESPACE` to perform cnDBTier procedures which wiped out CNE resources. To inform users to perform steps only on cnDBTier namespace, notes are added in the cnDBTier documents wherever necessary.	3	23.4.0
35657461	Multiple Restarts observed in ndbmysqld pods during upgrade to 23.2.1	Replication SQL pod restarted before it came up and connected to the cluster when Aspen Mesh service was enabled.	3	23.2.1
36242316	DBTier DR Script failing, unexpected number of server IDs	User requested to document the procedure to remove a site from a cnDBTier deployment. For the procedure to remove a site from a cnDBTier deployment, see Oracle Communications Cloud Native Core, cnDBTier User Guide.	3	23.2.2
36225991	Restart observed in all replication svc pods while deploying a 3 site 6 channel setup	User requested to add startup probe waiting time parameters in the `custom_values.yaml` file for the replication service pod.	3	23.4.0
36204471	On asm enabled setup on executing dbtrecover config details are not displayed	The `dbtrecover` script failed to determine if HTTPS and database encrypt features are enabled in ASM clusters.	3	23.4.0
36265057	Error logs observed on terminal when password script is executed with actual NF	Error logs were observed while running the `dbtpasswd` script. The `dbtpasswd` script is enhanced to provide better error handling and to roll back changes when an error occurs.	3	23.4.0

Table 4-9 (Cont.) cnDBTier 23.3.3 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34997129	Clarification on DBTier Automated Backup behavior	The timezone for the backup manager service and the executor service had to be changed to UTC timezone.	3	22.4.0
36363119	Post restart nbdmtd is not able to come up	The `nbdmtd` pod was unable to come up after a restart.	3	23.2.2

Table 4-10 cnDBTier 23.3.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35956435	Cluster failure on Mansfield Voice PCF	The `TimeBetweenWatchDogCheck` parameter had to be added and set to "800" for cnDBTier data node configuration.	1	23.2.1
35701853	Unable to run dbtrecover script on a setup deployed with encryption enabled	The `dbtrecover` script did not support encryption. As a result, the script was not able to perform georeplication recovery on setups where encryption is enabled.	2	23.2.1
35899529	PCF is not sending N28 or N36	Database replication service failed to restart all the `ndbappmysqld` pods after the georeplication recovery was complete.	2	23.1.3
35913453	DR stuck in INITIATEBACKUP state if remote transfer has failed	Database backup manager service did not take any new backup if the backup transfer from one data pod to replication service failed.	2	23.3.0
35516058	Freshly installed 4 site 6 channel setup not stable - mySQLD pods restart due to binlog thread crash	Database monitor service restarted the replication SQL pods while installing cnDBTier even when the binlog threads were not crashed.	2	23.2.0
36085415	Restart in SQL pods on Scaling down and up replicas of all Replication services	Database monitor service restarted the replication SQL pods while installing cnDBTier even when the binlog threads were not crashed.	2	23.4.0

Table 4-10 (Cont.) cnDBTier 23.3.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35956635	Geo-Replication Recovery failed in a 4 site setup with 1 other site FAILED	Georeplication recovery failed as the process was stuck in the BACKUPRESTORE state and then in the RECONFIGURE state.	2	23.2.1
35600314	Password Change script fails on Single site setup	The `dbtpasswd` script failed on single site setups. The `dbtpasswd` script had some issues that needed a fix.	2	23.2.0
35592603	Replication breaks on MultiChannel setup after password change is performed	The `dbtpasswd` script failed on multi-channel setups. The `dbtpasswd` script had some issues that needed a fix.	2	23.2.1
35789744	Unable to run recovery on a 4 site multi channel setup using dbtrecover script	The `dbtpasswd` script failed when the number of replication SQL pods was greater than 10.	2	23.3.0
35913287	Remote transfer fails as backup transfer from data to replication svc failed	The backup manager service was not able to resend the backup file if there was a deadlock in one of the executor services.	2	23.3.0
35906173	Timeout observed in Upgrade during Horizontal scaling procedure of ndbappmsyqld pods	Helm upgrade timed out when it was run in parallel with autoscaling of `ndbappmysqld`.	3	23.3.0
35805494	DBTier performance following traffic migration	Database monitor service (db-monitor-svc) failed to run some queries.	3	22.4.0
36103499	Command to kill the replication svc container is failing in dbtrecover execution	When SSH connection was established, orphan processes were displayed in the database replication service pod.	3	23.4.0
35504646	Unable to run recovery via dbtrecover script on an HTTPS enabled setup	The `dbtrecover` script failed to work when https connection was enabled between two sites.	3	23.2.0
36121890	cndbtier_restore.sh statefulsets.apps "ndbmysqld" not found	The `cndbtier_restore.sh` script failed to run some commands if the statefulset names had prefix.	3	23.2.0

Table 4-10 (Cont.) cnDBTier 23.3.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36000990	Temporary errors observed during DB restore	cnDBTier documentation had to be updated with a note to ignore temporary errors that are observed while restoring a database.	3	23.3.1
35456588	DBTier 23.1.0: Need an update on documentation of the cnDBTier Alerts	The alert documentation in the user guide had to be updated to provide details about the recommended actions for each alert.	3	23.1.0
36089914	Query regarding "REPLICATION_SKIP_ERRORS_LOW" alert	The `REPLICATION_SKIP_ERRORS_LOW` alert did not get cleared after the default time limit of one hour.	3	23.1.2
34646876	User guide update with an architecture diagram and short description of services	cnDBTier user guide had to be updated to provide details about cnDBTier architecture and microservices.	3	22.1.0
35973810	cnDBTier 23.2.2 and 23.3.x has % missing as special character in the mksecrets.sh script	The `mksecrets.sh` script had to be updated to support the "%" character in MySQL passwords.	3	23.2.2
35600316	Password change script seems to get stuck	The `dbtpasswd` script got stuck randomly at some point while performing a password update.	3	23.2.0
36107599	Unable to recover 2nd site when using dbtrecover	The `dbtrecover` script was unable to recover the second fatal error site.	3	23.4.0
35975443	Error logs being printed in db-executor svc	Unnecessary error messages were printed in database backup manager service logs when there was no backup to purge.	4	23.3.1
36030365	cnDBTIer 23.3.0 - DR Guide Refinement Request, re: 4-Site Geo-Replication	Georeplication recovery procedures in *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide* required certain updates and corrections.	4	23.3.0

Table 4-10 (Cont.) cnDBTier 23.3.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36043512	Correct spellings of logging in dbtrecover logs	`dbtrecover` logs had certain spelling errors which required correction.	4	23.2.3
36146937	cnDBTIer 23.4.0 - DR Guide Refinement Request: 7.4.9.1 Procedure Point 2.d	The steps to get the Load Balancer IPs in the cnDBTier georeplication recovery procedures documented in *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide* had to be updated with the correct description.	4	23.4.0

Table 4-11 cnDBTier 23.3.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35410102	DR failure due to error : remotesitedatanodecount.properties does not exists	Georeplication fault recovery failed as `/var/occnedb/dbbackup/remotesitedatanodecount.properties` got removed when the backup transfer failed once and was retried.	2	23.1.1
35754271	Drastic increase in size of mysqld.log file on 23.3.0	Drastic increase in the size of the mysqld.log file was observed on cnDBTier 23.3.0. The issue was caused by the warning messages generated by MySQL for using deprecated authentication plugin.	2	23.3.0
35812585	DR got stuck when we executed it on upgraded setup from 23.1.2 to 23.3.0	Georeplication recovery got stuck if ndb_cluster_connection_pool was set to a value more than "1".	2	23.3.0
35848919	Connectivity fails towards "running" ndbappmysqld pods' mysql-server during upgrade . Behaviour not seen during pod termination.	During an upgrade, ndbappmysqld pods came to the running state before the MySQL process was ready leading to connectivity failure.	2	23.3.0

Table 4-11 (Cont.) cnDBTier 23.3.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35789704	During rollback of CNDB from 23.2.1 to 23.1.1, replication breaks and db-backup-manager pod is stuck in crashloopbackoff	*Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide* had to be updated with a note stating that two hop rollback with different versions is not supported by MySQL and cnDBTier.	2	23.1.1
35740004	DBTier Installation Guide: SiteId in the yaml file need to be set as 1, 2, 3, 4	The `SiteId` parameter in the YAML file must be set as 1, 2, 3, and 4 for one, two, three, and four sites respectively. This condition is updated in the parameter description in *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*.	2	23.1.0
35724053	cnDBTier 22.4.3 db_tier_backup{status="FAILED"} prometheus alert	Old backup failure alerts were not cleared by the cnDBTier code.	2	22.4.3
35895036	On-demand Backup fails on a single site CNDB 23.3.0	On demand backups failed on a single site setup if the replication service pod was not present.	2	23.3.0
35592603	Replication breaks on MultiChannel setup after password change is performed.	Replication broke on multichannel setups after a password change due to issues in the dbtpasswd script.	2	23.2.1
35600314	Password Change script fails on Single site setup	The dbtpasswd script failed on single site setups.	2	23.2.0
35817717	Incorrect format of remote backup file.	The details about the file name and path in which the backups are stored in remote servers were missing in *Oracle Communications Cloud Native Core, cnDBTier User Guide*.	3	23.3.0

Table 4-11 (Cont.) cnDBTier 23.3.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34997129	Clarification on DBTier Automated Backup behavior	The time zone of db-backup-manager-svc and db-backup-executor-svc was required to be changed to the UTC format.	3	22.4.0
35372063	Skip error feature for CNDBTier not working when using site id as 5 and 6 for a 2 site GR setup.	The skip error feature didn't work as the server IDs were configured incorrectly. To fix this issue, the equation to create server ID was added to the server ID parameters in Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide.	3	23.1.0
35504362	Replication svc pvc is not getting recreated on pod deletion, if in state of termination	*Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide* needed to be updated with the procedure to handle single node recovery for replication service.	3	23.1.1
35829082	REPLICATION_SKIP_ERRORS_LOW alarm is firing for cnDBTier	The REPLICATION_SKIP_ERRORS_LOW alarm was not getting cleared after the default time limit due to incorrect configurations. The alert documentation in Oracle Communications Cloud Native Core, cnDBTier User Guide is updated with the detail that the alert gets cleared after the time limit of one hour.	3	23.2.1
35727796	Document steps to recover all sites if all sites are down is missing	*Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide* needed to be updated with the fault recovery procedure to recover all sites if all sites are down.	3	23.2.0

Table 4-11 (Cont.) cnDBTier 23.3.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35798774	CNDBTier 23.3.0 Installation is failing via CDCS	cnDBTier installation failed when the installation was performed through CDCS due to CNE compatibility issue in generic CSAR.	3	23.3.0
35600316	Password change script seems to get stuck	The dbtpasswd script failed on four-site setups.	3	23.2.0
35906173	Timeout observed in Upgrade during Horizontal scaling procedure of ndbappmsyqld pods.	Helm upgrade failed while performing a horizontal scaling of ndbappmsyqld pods as max_wait was static.	3	23.3.0
35909630	cnDBTier 23.2.1 software packaging issue	The occndbtier_mysqlndb_vnfd.yml file in the CSAR package was incorrect.	3	23.2.1
35432969	Listing the changes made in the CNDBTIER MOP 22.4.2 for engineering approval	The MoP documentation for 22.4.2 and the user documents were not in sync.	4	22.4.2

Table 4-12 cnDBTier 23.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35447967	DBTier_Upgrade: Data pod in "CrashLoopBackOff" observed during cndb upgrade from CNDB_23.1.0 to CNDB_23.2.0 & Error: 2308 shown	While upgrading cnDBTier, the data pods ran into CrashLoopBackOff state with an 2308 error code. It was observed that changing the value of HeartbeatIntervalDbDb from 5000(ms) to 500(ms) in one step resulted in this issue. To resolve the issue, the upgrade procedure is modified with the steps to update the HeartbeatIntervalDbDb value from 5000(ms) to 500(ms) in multiple steps.	1	23.2.0

Table 4-12 (Cont.) cnDBTier 23.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35457407	GR Break observed for Site3 in a 4 Site GR setup post traffic run.	Replication broke on cnDBTier setups where the MTA feature was enabled. Therefore, MTA is disabled until the issues are resolved and the installation and upgrade procedures are updated with notes to disable the MTA feature.	2	23.2.0
34618463	Horizontal Scaling of ndbmtd pods	Multiple restarts and cluster disconnects were observed while performing horizontal scaling of ndbmtd pods. The issue was due to deleting the data nodes in ascending order instead of following a descending order.	2	22.3.0
35410102	DR failure due to error : remotesitedatanodecount.properties does not exists	Georeplication fault recovery failed as `/var/occnedb/dbbackup/remotesitedatanodecount.properties` got removed when the backup transfer failed once and was retried.	2	23.1.1
35642153	cnDBTier v23.2.0 ndbmtd pods were in crashLoopBackoff status after deploy	The PVC monitoring feature increased the PVC load in cnDBTier. As a result, the ndbmtd pods went into the crashLoopBackoff status after deployment.	2	23.2.0
35677152	DR Stuck in INITIATEBACKUP; Failed to create a file, filename: backup_encryption_password	While performing a replication recovery of a site, the dr_state got stuck at INITIATEBACKUP state as the system was unable to create the backup_encryption_password file. It was observed that the "backup_encryption_password" file was already present in the pod.	2	23.2.1
35643518	Channel switchover leading to replication break on multi channel setup	Switchover failed to resume when it encountered a REST API timeout scenario due to network delays.	2	23.2.1

Table 4-12 (Cont.) cnDBTier 23.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35249321	Automatically purge some binlog on startup if it is full to avoid pod going in crashloopbackoff state	The delta binary logs had to be automatically purged on startup if the PVC was full to avoid the pod from going in the crashloopbackoff state.	3	22.4.1
35297954	Response of Fault Recovery APIs should be in JSON format instead of plain text for negative Error code	The user requested to modify the response content-type of the fault recovery APIs from application/json to application/ problem+json.	3	23.1.0
35526956	Metric for db-infra-monitor svc not documented in User Guide	The user requested to document the metric and alert for the PVC health monitoring in the user guide.	3	23.2.0
35564236	Alert to monitor PVC health are not implemented in 23.2.0	The user requested to create alerts for the PVC health monitoring metrics and update the user guide accordingly.	3	23.2.0
35523597	cnDBTier MoP Updates:steps for ndbappmysql pod scaling with service accout and autoscaling disabled	The user requested to include the missing sections for the ndbappmysqld horizontal scaling procedure in cnDBTier User Guide.	3	23.1.1
35395995	Alert BINLOG_STORAGE_FULL since installing 22.3.2	The user requested to raise a BINLOG_STORAGE_FULL alert when apiReplicaCount is 0 and replication SQL PVC is set to 0.	3	22.3.1
35364251	DBTier 22.4.1 alert's expression issues	Customer requested to clear the `REPLICATION_SWITCHOVER_DUE_CLUSTERDISCONNECT` alert after a fixed time.	3	22.4.1
35611594	Cleanup did not happened in data pods when DR failed	When a backup transfer failed, the backup tar files created by the process were not cleaned up.	3	23.2.0
35561614	DBTier 23.2.0 high number of writes when Inframonitor PVC Health Enabled	The PVC monitoring feature caused a high number of disk writes and increased the PVC load in cnDBTier.	3	23.2.0

Table 4-12 (Cont.) cnDBTier 23.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35527785	mksecrets.sh script name is mentioned wrongly in the cnDBTier installation guide	The name of the mksecrets.sh script was incorrect in the cnDBTier installation guide.	4	23.2.0
35569579	File name should be updated in 23.2.0 Post Install Guide	Grafana and alert rule file names in the post installation procedures were to be updated as per the latest build.	4	23.2.0
35667464	Correct panel locations for Infra Health Monitor Metrics	PVC monitoring Grafana dashboards were not present in the correct location.	4	23.2.1
35681525	Correction needed in spelling in replication service logs	There was a typo in the replication service log (log0) message.	4	23.2.1

Note:

Resolved bugs from 22.4.3, 23.1.2, and 23.2.1 have been forward ported to Release 23.3.0.

4.2.5 NEF Resolved Bugs

Table 4-13 NEF 23.3.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36123196	Forbidden! Configured service account doesn't have access. Service account may have been revoked during In Service Upgrade	The configured service account did not have access because it might have been revoked during the service upgrade.	3	23.3.0

Table 4-14 NEF 23.3.1 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 that include an External Group ID were receiving the following error:	3	23.2.0

Table 4-14 (Cont.) NEF 23.3.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35779947	AEF-API Router's config map of NEF is unable to retrieve the changes after adding the parameter apiPrefix (as 'apiRoot')	The AEF-API Router's config map of NEF was unable to retrieve the changes after adding the parameter apiPrefix as 'apiRoot'.	3	23.3.0

Table 4-15 NEF 23.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35564254	NEF-GR-Site: 0.5ktps - Replication status Down during NEF upgrade from 22.4.3 to 23.2.0	While upgrading NEF from 22.4.3 to 23.2.0, the ME services hooks were triggering many ALTER (DDL) statements on ocnef_me_subscription table.	1	23.2.0
35526054	NEF-GR Site :0.5Ktps traffic - Site1 and Site2 traffic Loss rate is more than 1% during NEF Rollback from 23.2.0 to 23.1.2	While performing Site2 to NEF2 rollback, there was 98.7% success rate and 1.29% loss rate. Similar behavior is observed during Site1 to NEF1 rollback, with more than 1% loss rate.	2	23.2.0
35523391	NEF-GR Site :0.5ktps traffic - Site1 traffic Loss rate is more than 1% during Site1 - NEF1 upgrade from 23.1.2 to 23.2.0	While performing Site1 to NEF1 upgrade, there was 98.8% success rate and 1.17% loss rate.	2	23.2.0
35753428	GR Setup: NEF:23.3.0_RC5: 100% subcrption loss observed after capif upgraded from 23.2.0 to 23.3.0_RC5 build	During capif1 upgrade from 23.2.0 to 23.3.0 rc5 build, it was observed that there was 99.99% success rate and post 30 minutes of upgrade there was 100% subscription loss.	2	23.3.0
35646946	NEF:TLS-GR : Traffic Influence(TI) subscription with TLS enable (https) failed with some of the NF's interaction.	While creating TI subscription, the parameters such as IP, externalgroupid, and UE indication were rejected.	2	23.2.0
35429399	Model -B : TI subscription: gNbId object with bitLength parameter is not available in geoZoneIdToSpatialValidityMap configuration.	While creating TI subscription, it was observed that the gNbId object with `bitLength` parameter was not available in `geoZoneIdToSpatialValidityMap` configuration.	3	23.1.0
35385035	Latency of UDM and GMLC unsubscription's is getting increased in the long performance run of ME scenarios.	While performing long performance run of ME scenarios, latency of UDM and GMLC unsubscription increased.	3	23.1.2

Table 4-15 (Cont.) NEF 23.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35311912	TI subscription:-Trafficroutes with invalid ipv6 address and invalid ipv6 format is subscribed.	While creating TI subscription, it was observed that the traffic routes with invalid IPv6 address and invalid IPv6 format were subscribed.	3	23.1.0
35294019	SNSSAI value is not hexadecimal in NEF yaml file	In NEF custom yaml file, it was observed that the SNSSAI value was not in hexadecimal format.	3	23.1.0
35593684	NEF-ATS: 23.2.0 :- NEF stubs are going terminated loop after enabling https parameter.	While installing stubs package, only UDM pod was in running state and all other pods were going for terminated loops.	3	23.2.0
35593125	NEF :TLS enable :- Configuration of NRF registration using (prioritizeServiceFqdnOverProfileFqdn) parameter not available in the ocnef-custom yaml file.	While registering to NRF, the `prioritizeServiceFqdnOverProfileFqdn` parameter required for configuration was not available in the ocnef-custom yaml file.	3	23.2.0
35592833	NEF-ATS :23.2.0- TLS enabled https messages rejected by UDM stubs.	While triggering ME subscription, UDM stubs rejected the TLS enabled messages.	3	23.2.0
35274378	Traffic influence with same ipv6 address with differnt format allowing subscription	While creating TI subscription, if ':' format (example: 2010:0000:0000:0000:0000:0000:0000:0002) is used, then it should be rejected. It was identified that the wrong format was not being rejected.	3	23.1.0
35621221	Capif -TLS enable : During Pre Provisioning AF, onboardinguri sending "http" instead of "https".	While performing pre-provisioning of AF stage, the `onboardingUri` parameter was sending http instead of https.	3	23.2.0
35604266	NEF should support MSISDN value of 5-15 digits in subscription request but currently it is supporting 6-16 digits	While subscribing, NEF should support MSISDN value of 5-15 digits, but it was observed that it supported 6-16 digits.	4	23.2.0

4.2.6 NRF Resolved Bugs

Table 4-16 NRF 23.3.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
36215562	NRF rejects the discovery query when “allowedPlmns” does not contain the PLMN in the registration profile	The PLMN ID(s) registered in the NF profile were not considered while allowing to access the NF service instance when the allowedPlmns attribute is present at the NFservice level.	2	23.2.1
36128595	NRF 23.2.0 SCP monitoring via SCP Health APIs Fails on HTTP	HTTP Option packets were not seen in the PCAP. The handshake worked fine with SCP and the only impact is the packet is not decodable.	2	23.2.0
36215509	Logs are getting incorrectly reported as ERROR causing flooding of logs in NRF 23.2.2 Discovery pods.	Incorrect logs were generated when target nftpye is UDR, UDM or any NF type that contained supi as a query parameter. The logs were flooded in the discovery pods, which might exhaust the ephemeral storage of the pod leading to downtime of these pods.	3	23.2.2
36215642	Metrics has nfFqdn dimension incorrect	A list of metrics gets pegged in NRF with nfFqdn dimension as "nfFqdn" (hardcoded). It should peg the value as received in the XFCC header (if the feature is enabled).	3	23.4.0
36215740	ocnrf_replication_status_total does not get pegged on nrfArtisan service	ocnrf_replication_status_check_total does not get scrapped from the artisan pod due to which OcnrfReplicationStatus MonitoringInactive alert will be raised for the pod even if replication is up.	3	22.3.2
36215820	indentation issue as whitespace character got substituted by tab unintentionally - broke yaml lint	There were indentation issues as the whitespace character was substituted by tab unintentionally which caused the upgrade/ rollback failure with yaml lint error.	3	23.2.2

Table 4-16 (Cont.) NRF 23.3.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
36215843	NRF is not updating NFServiceListMap in case priority is getting updated in NFService level during preferred locality features	When extended preferred locality feature updated the priority/load of the profiles as per the configuration, NRF only updated the priority present in nfService attribute of the profile. nfServiceListMap attribute is sent as received during registration.	3	23.2.2
36179824	NRF-ATS 23.3.1 - Service Account creation issue for STUB installation in NRF-ATS 23.3.1	There was no Service Account parameter in the ATS values.yaml file for Stubs, and it created a default service account. For deployments, where Service Account needs to be provided at the time of deployments, there was no option available to provide the same.	3	23.3.1
36052221	NRF 23.3.2: NRF 23.3.0 is getting upgraded successfully during post upgrade validation when table is missing or schema is incorrect for NfSubscription or NfRegistration Microservices.	NRF upgrade did not fail when table was missing or the schema was incorrect for NfSubscription or NfRegistration Microservices.	3	23.3.1

Table 4-16 (Cont.) NRF 23.3.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
36242707	Alerts Firing Due To Multiple nrfAuditor Pods	Deployments operating with more than one nrfAuditor pod will fire alerts for conditions that do not exist due to non-Leader nrfAuditor pod returning a value of 0 for certain metrics. For example, Critical Alert OcnrfRegisteredPCFsBelowCriticalThreshold does not fire for the NRF's nrfauditor pod identified as Leader (as determined by table leaderElectionDB.NrfAuditorLeaderPod) when the nonzero value based on scraped metric ocnrf_active_registrations_count is returned from that pod. However, every non-Leader nrfauditor pod will return a value of "0" for that metric and consequently the Alert expression will trigger the Alert.	3	22.3.2
36242721	Jaeger tracing attributes of common services like ingress gateway, egress gateway not updated from openTracing to openTelemetry	NRF has migrated to OpenTelemetry , however the configurations still pointing to OpenTracing.	3	23.3.1
36215740	ocnrf_replication_status_total does not get pegged on nrfArtisan service	`ocnrf_replication_status_check_total` does not get scrapped from the artisan pod due to which OcnrfReplicationStatusMonitoringInactive alert will be raised for the pod even if replication is up.	3	22.3.2

Table 4-17 NRF 23.3.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
35830391	Incorrect x5c header type(string) in jwt token implemented for NRF feature CCA Header Validation	The x5c header in jwt token implemented for the CCA Header Validation feature in NRF had incorrect data type as string. This data type is changed as an array.	2	23.2.0
35830516	UDM patch request to update "serviceInstanceId" gets rejected by NRF	UDM patch request sent to update the `serviceInstanceId` was rejected by NRF. Upon resolving this issue, the `serviceInstanceId` is now not rejected by NRF and is processed by NRF.	2	23.2.0

Table 4-18 NRF 23.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
35654615	NRF is sending NFStatusNotify message for AMF updates NOT within the same AMF set (amfSetId+amfRegionId)	As per 3GPP TS 29.510, NRF should send a notification when both `amdSetId` and `amfRegionId` conditions are met. NRF was only checking for matching `amfSetId`, whereas it should check for both `amfRegionId` and `amfSetId` before sending the NFStatusNotify message.	2	22.4.2
35140199	NRF microservices pods like Accesstoken, Registration, Discovery restarts were observed during NRF upgrade from 22.4.1 to 23.1.0.	NRF microservices pods such as Accesstoken, Registration, and Discovery restarted during NRF upgrade from 22.4.1 to 23.1.0 because Kubernetes configuration inside microservices was not loaded before access.	2	23.1.0
35752960	NRF 23.1.1 closing active TCP connections after 2 mins	NRF 23.1.1 was closing active TCP connections after 2 mins.	2	23.1.1

Table 4-18 (Cont.) NRF 23.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
34955154	Performance info pods gets restarted multiple times during upgrade procedure	Performance info pods restarted multiple times during the upgrade procedure in an ASM enabled setup.	2	22.4.0
35603685	isIpv6Enabled flag is missing in egressGateway configuration causing 400 Bad Request for IPv6 request	`isIpv6Enabled` flag was missing in Egress Gateway configuration which caused 400 Bad Request for IPv6 request.	2	23.2.0
35726724	NRF Installation failing while doing the NRF fault recovery for Scenario: Deployment Failure (NRF Corruption) with global.appValidate.faultRecoveryMode parameter set to true.	NRF installation failed while performing the NRF fault recovery when the *global.appValidate.faultRecoveryMode* was set to true.	2	23.2.0
35752651	NRF is including the interPlmnFqdn attribute in NFProfile during NFStatusNotify messages	As per 3GPP TS 29.510, `interPlmnFqdn` attribute in NFProfile must not be in NFStatusNotify messages.	3	23.1.1
35433885	NRF ATS 23.2.0 New Features testcase fails for SCP monitoring	SCP monitoring failed due to stale data configuration in the Egress Gateway.	3	23.2.0
35545870	Request metrics for NSI and Snssai Discovery is not inline with other discovery metrics	The metrics names for NSI and SNSSAI discovery request messages were incorrect in the metric dashboard and documentation.	3	23.2.0
35752981	Network Policy - Add policy for CNCC and Notifications from OCNRF	Network Policies must include policy for CNCC and notifications from NRF.	3	22.4.0
35753034	NRF is taking value from user agent header rather from Access Token request json	While processing AccessToken request, NRF took value from User-Agent Header instead of Access Token request json.	3	23.1.0
35561513	NRF ATS test cases failing in PI-B CY23 due to Timeout exception in egress gateway for unknown host	NRF ATS test cases failed due to Timeout exception in Egress Gateway for unknown host.	3	23.2.0

Table 4-18 (Cont.) NRF 23.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
35754205	NRF respoding with 200 OK constantly for Heatbeat change for load.	NRF should not send 200 responses for every change in load in the Heartbeat message. Load changing was a normal phenomenon of NF which should not warrant sending a 200 response with a full NfProfile.	3	23.1.1
35754314	Heartbeat: Load attribute in nfServiceList need to be considered as Heartbeat like with NFStatus and Load at NFprofile and NFservice	Load attribute for `NfServices` in `nfServiceList` attribute was not considered as Heartbeat, for example, NFStatus and Load at NFprofile and NFservice.	3	23.1.1
35656055	NfProfile is being saved with NRF with port: 0 if port is absent in ipEndPoints	NfProfile was saved with NRF with port: 0, if port was not provided in the ipEndPoints.	3	23.2.0
34844121	NRF Auditor: Install hook and auditor service are taking leaderElectionDbName from different places	Install hook and auditor services were taking leaderElectionDbName value from different configurations. Install hooks were taking the leaderElectionDbName value from the secret but Auditor logic was taking database name from values.yaml.	3	22.3.1
35562113	Metric "ocnrf_nfDiscovery_tx_success_response_perSnssai_total" and "ocnrf_nfDiscovery_tx_success_response_perNsi_total" are not pegged in forwarding scenarios.	The following metrics did not peg during forwarding scenarios: • `ocnrf_nfDiscovery_tx_success_response_perSnssai_total` • `ocnrf_nfDiscovery_tx_success_response_perNsi_total`	3	23.2.0

Table 4-18 (Cont.) NRF 23.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
35595721	Metric "ocnrf_nfDeregister_requests_perSnssai_total" and "ocnrf_nfDeregister_success_responses_perSnssai_total" are not pegged in case of sNssaiSmfInfoList in SMF profile	The following metrics did not peg in case of sNssaiSmfInfoList in SMF profile: • `ocnrf_nfDeregister_requests_perSnssai_total` • `ocnrf_nfDeregister_success_responses_perSnssai_total`	3	23.2.0
35625097	Heartbeat and update requests and responses metrics per snssai not getting pegged in case of sNssaiSmfInfoList in SMF profile.	Heartbeat and update requests and responses metrics per snssai did not peg in case of sNssaiSmfInfoList in SMF profile.	3	23.2.0
35465622	Standby Auditor pod is not picking log level change	Standby Auditor pod did not pick the log level changes from the database.	3	22.3.2
35671686	After removing SCP peer configuration NfStatusNotify requests goes via SCP.	Even after removing SCP peer configuration, `NfStatusNotify` requests were routed through SCP. The requests were not redirected to the default route.	3	23.2.0
35755584	Metric "ocnrf_nfDiscovery_tx_success_response_perSnssai_total" is getting pegged as "ocnrf_nfDiscover_tx_success_response_perSnssai_total"	"`ocnrf_nfDiscovery_tx_success_response_perSnssai_total`" metric was incorrectly pegged as "`ocnrf_nfDiscover_tx_success_response_perSnssai_total`".	3	23.2.0
35635787	HB response metric is pegged with incorrect response code	HeartBeat response metric was pegged with an incorrect response code.	4	23.2.0
35701152	Incorrect value mentioned for default parameters of NRF Peer Monitoring Configuration in REST API GUIDE section 5.8 Peer Monitoring Configuration	Incorrect value was mentioned for default parameters of NRF Peer Monitoring Configuration in *Oracle Communications Cloud Native Core, Network Repository Functions REST Specification Guide*.	4	23.2.0

Table 4-18 (Cont.) NRF 23.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
35755613	NRF- validationRule when set to "relaxed" NRF stop rejecting invalid IssuedAt parameter in CCA header for feature - CCA Header Validation	NRF validationRule was set to "relaxed", hence NRF was not rejecting invalid IssuedAt parameter in CCA header.	4	23.2.0
35755694	snssais of NfService/ NfServiceList is not pegged in NRF operations request metric must be documented in user guide	snssais of NfService/ NfServiceList was not pegged in NRF operations request metric.	4	23.2.0
35755714	NRF- Change in value for configuration parameter "subKey" does not work in feature - CCA Header Validation	CCA Header Validation feature didn't work when the value of configuration parameter "subKey" was modified.	4	23.2.0
35755727	NRF- Incorrect metric name oc_egressgateway_sni_error in user guide for NRF feature - TLS SNI	Incorrect metric name `oc_egressgateway_sni_error` was documented for TLS SNI feature in *Oracle Communications Cloud Native Core, Network Repository Functions User Guide*.	4	23.1.0

4.2.7 NSSF Resolved Bugs

NSSF 23.3.1 Resolved Bugs

There are no resolved bugs in this release.

Table 4-19 NSSF 23.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35673227	During deployment nsavailability pod is not coming up on disabling ONSSAI, SUMOD, EANAN & ES3XX	After the successful run of the deployment edit command for "nsavailability," and after setting ONSSAI, SUMOD, EANAN, and ES3XX to "false" within the "nsavailability" deployment, the "nsavailability" pod did not come up.	2	23.2.0

Table 4-19 (Cont.) NSSF 23.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35572519	The CPU Quota and Limit Range in deployment cannot be changed once NSSF CPU Quota and Limit Range have been exceeded.	The CPU Quota and Limit Range in the deployment couldn't be changed after the NSSF CPU Quota and Limit Range exceeded.	2	23.2.0
35617375	NSSF 23.2.0 Availability Update Latency - Request Timeout at IGW	Latency exceeded by 6 seconds while processing an availability update request. An error was also found in the Ingress Gateway log, indicating a request timeout.	2	23.2.0
35498940	In Service Solution rollback: 2 Site GR Setup, Ingress failure (4.219% dropped on Site-2 and 5.607% dropped on Site-1) observed during in service solution rollback both sites from CNDB version 23.2.0 to 23.1.1	While performing in-service rollback on two-site GR setups, ingress failure was observed with a drop rate of 4.219% on site-2 and 5.607% on site-1. This problem occurred while rolling back cnDBTier version from 23.2.0 to 23.1.1.	2	23.2.0
35498800	In Service Solution Upgrade: 2 Site GR Setup, Ingress failure (3.306% dropped on Site-1) observed during site 1 in service solution upgrade from CNDB version 23.1.1 to 23.2.0	While performing in-service upgrade on two-site GR setups, ingress failure was observed on site-1 with a drop rate of 3.306%. This issue occurred while upgrading cnDBTier version 23.1.1 to 23.2.0.	2	23.2.0
35566080	2-site GR setup ASM Enabled: Failover : Site-2 success rate dropped by 0.18% for 2 hours and success rate dropped by 5.661% for 7 hours during failover	During the two-site GR setup with ASM enabled, a failover event was observed. The success rate for site-2 experienced a decrease of 0.18% over a span of 2 hours. Additionally, the success rate dropped by 5.661% over a duration of 7 hours during the same failover period.	2	23.2.0

Table 4-19 (Cont.) NSSF 23.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35488386	In Service Upgrade: 2 Site GR Setup, subscription pod is not coming up because of NotificationTrigger.getTai() is null	During in-service upgrade with a two-site GR Setup, the subscription pod failed to start. This indicated that the NotificationTrigger.getTai() was returning a null value.	2	23.2.0
35498983	In Service Solution rollback : 2 Site GR Setup, Ingress failure (1.123% dropped on Site-1 and 2.655% dropped on Site-2) observed during in service solution rollback both sites from NSSF version 23.2.0 to 23.1.1	During in-service rollback with a two-site GR setup, ingress failure was observed with a drop rate of 1.123% on site-1 and a drop rate of 2.655% on site-2. This issue occurred while rolling back cnDBTier version from 23.2.0 to 23.1.1.	2	23.2.0
35476642	In NSSF 23.2.0, 10K performance long run (2.5 days approx.), traffic dropped because of http code 500.	In NSSF version 23.2.0, during a performance test spanning for approximately 2.5 days, a significant traffic drop was observed due to HTTP code 500 error.	2	23.2.0
35476746	In NSSF 23.2.0, 10K performance long run (2.5 days approx.), average latency of scenarios are 220 ms.	In NSSF version 23.2.0, during a performance test that was run for around 2.5 days, the average latency for various scenarios was measured at 220 ms.	2	23.2.0
35568608	2-site GR setup ASM Enabled: Site Restore : Restoration of Replication not working after 7 Hours Failover Execution	In a two-site GR setup with ASM enabled, an issue was observed while restoring the replication functionality. This problem occurred after running the failover for 7 hours.	2	23.2.0

Table 4-19 (Cont.) NSSF 23.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35565882	2-site GR setup ASM Enabled: Split-Brain: Site-1 success rate dropped 25% after Split Brain recovery and during split brain success rate dropped 7.11%	In a two-site GR setup with ASM enabled, a Split-Brain scenario occurred when replication channel was down for 90 minutes. During the Split-Brain situation, there was a drop of 7.11%. in the success rate. After the replication channel restarted, the site-1 experienced a drop of 25% in the success rate.	2	23.2.0
35553199	2-site GR setup ASM Enabled: success rate dropped 0.49% on site 2 during traffic run 5K on each site approx. 40 hours	In a two-site GR setup with ASM enabled, a success rate drop of 0.49% was observed on site-2 during a traffic run of approximately 5,000 requests on each site for 40 hours.	2	23.2.0
35522976	Egress pod having error "Unhandled exception occured" and NSSF showing wrong Peer health info (Support for SCP Health API using HTTP2 OPTIONS)	The egress pod experienced an 'Unhandled exception occurred' error, and incorrect peer health information was displayed when 'peermonitoringconfiguration' and 'SBI Routing' were enabled.	3	23.2.0
35635322	Subscription happen successful with Invalid binding header "Indirect Communication" with NSSF 23.2 while expected is 400 Bad request	The subscription was successful, but an invalid binding header "Indirect Communication" was received from NSSF version 23.2.0 instead of a "400 Bad Request" error.	3	23.2.0
35503266	NSSF provide peer health info as healthy even after peer monitoring feature is disable (Support for SCP Health API using HTTP2 OPTIONS)	When 'SBI Routing' and 'peermonitoringconfiguration' were enabled, even after disabling peer monitoring, the NSSF incorrectly reported peers as healthy when using the SCP Health API with HTTP2 OPTIONS.	3	23.2.0

Table 4-19 (Cont.) NSSF 23.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35667809	Not getting HTTP 403 Unsupported PLMN Error Details instead getting 422 error code on tac mismatch with PLMN	The expected HTTP 403 "Unsupported PLMN" error details were not received. Instead, a 422 error code was received when there was a TAC (Tracking Area Code) mismatch with the PLMN (Public Land Mobile Network).	3	23.2.0
35469159	NSSF 23.1.1 installation issue Limit Range error	While installing NSSF version 23.1.1, a limitation range error was encountered in the "ocnssf-nsauditor" preinstall step.	3	23.1.1
35590843	NSSF 23.2: SUMOD Feature, Incomplete Answer	When performing an operation on a subscription in NSSF version 23.2.0, the response was incomplete. The expected changes in the "authorizedNssaiAvailabilityData" were missing from the response.	3	23.2.0
35570622	NSSF package's CNDB custom yaml should be CNDB 23.2.0 rather than 23.1.0.	The version of the `ocnssf_dbtier_23.2.0_custom_values_23.2.0.yaml` file in the NSSF package was 23.2.0 instead of 23.1.0.	3	23.2.0
35677480	NSSF 23.2 Stale subscriptions not getting deleted	Stale subscriptions were not automatically deleted.	3	23.2.0

Table 4-19 (Cont.) NSSF 23.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35368703	NSSF is not sending the taiRangeList in Notifications, if Ns-availability Update request for same taiRangeList	Following were the intermittent issues in scenarios where subscriptions included multiple TAI ranges and the configuration included intersecting TAI ranges: • When NsAvailabilityInfo included TAI ranges overlapping those in both the subscription and configuration, an error occurred. • When AMF represented the first instance to support a Ta-SNSSAI combination not backed by any other AMF in the network, the notification failed to capture this information.	3	23.1.0
35368636	NSSF is sending the Multiple Notifications, when Ns-availability Update request for same taiRangeList	Intermittent issues were observed when subscriptions included multiple TAI ranges and the configuration included intersecting TAI ranges. When the trigger for notification was NsAvailability info, NSSF sent multiple notifications instead of one.	3	23.1.0
35352648	NSSF is sending the failure for supportedNssaiAvailabilityData.taiRangeList.tacRangeList.pattern IE.	NSSF did not support optional parameter patterns that were included in TaiRangeList.	3	23.1.0
35395855	NSSF (Discovery request) is not retrying the discovery request towards NRF for failure scenario.	When configuring the AMF set, if a response from discovery resulted in an error and the MaxRetries parameter (Helm configuration) was set to 1, NsConfig did not trigger any retries.	3	23.1.0

Table 4-19 (Cont.) NSSF 23.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35377428	Unable to find out some subscription and discovery NRF metrics in prometheus	In one of the configuration scenarios, NSSF failed to peg a specific metric.	3	23.1.0
35396406	NSSF is sending the incorrect value of NRFNFmanagement IE and nrfAmfSetAccessTokenUri IE in ns-selection response.	In certain scenarios, NSSF failed to send the appropriate values for optional Information Elements (IEs) during the initial registration request.	3	23.1.1
35388661	NsAvailabilityInfo PUT call flow is taking more than 100ms	The flow of NsAvailabilityInfo PUT calls took more than 100ms.	3	23.1.1

Note:

Resolved bugs from 22.4.4, 23.1.0 , 23.1.1, and 23.1.2 have been forward ported to Release 23.3.0.

4.2.8 SCP Resolved Bugs

Table 4-20 SCP 23.3.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36240842	SCP does not pay attention to https schema in 3gpp-sbi-target-apiroot and try to setup http connection instead	SCP did not consider the https schema in the 3gpp-sbi-target-apiroot header and tried to set up an http connection instead of https to SMF.	2	23.2.3
36240917	Console SCP GUI - NF Instance Id and NF Type becomes non-editable fields which was editable before in nf Rule Profile screen	On the CNC Console, the NF Instance ID and NF Type fields have been disabled, however, these fields were enabled in the nf Rule Profile screen.	2	23.3.0
36240881	OCSCP metric pegged as NAN	This issue occurred when the measured object was dereferenced and the same object was metered again, then the underlying framework reported a NAN issue.	3	23.2.2
36240883	Static Routing configuration does not work when routeGroupType is FQDN	The static routing configuration did not work when `routeGroupType` was FQDN.	3	23.3.0

Table 4-20 (Cont.) SCP 23.3.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36240916	SCP sends incorrect LCI header format & payload in health check query response	SCP sent the incorrect LCI header format and payload in the health check query response.	3	23.3.0
36240944	SCP worker pod not coming up after upgrade from 23.2.1 to 23.3.1	The SCP-Worker pod was unavailable after upgrading from 23.2.1 to 23.3.1.	3	23.3.1
36240945	SCP accepts and establishes TLV v1.3 connection when TLSv1.3 is not officially supported	SCP accepted and established the TLV v1.3 connection when TLSv1.3 was not supported.	3	23.2.1
36240947	Syntax errors for SNMP trap MIB definition	Syntax errors were observed in the SNMP trap MIB.	4	23.2.0

Table 4-21 SCP 23.3.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36089521	scp_vnfd.yaml has incorrect mapping of multiple of charts under artifacts	The scp_vnfd file also had network policy charts listed under artifacts along with SCP charts. Thus resulting in deployment failure.	2	23.2.2
35817729	SCP-ATS:OutlierDetectionInterSCP.feature failed due to metrics mismatch	The virtual service (used by ASM sidecar) with attempted values set to 0 was not applied when using service mesh configuration deployment file.	2	23.2.2
35833224	SCP is rejecting Profile updates for FOREIGN SCP'	SCP was marking all the local SCP nfsetids as foreign when the notification pod was reinitialized, causing local SCP profile registration failure.	2	22.4.4
35829374	Invalid Api Version in response for notification call	API version was invalid in response to notification call-SCP 23.2.	2	23.2.0
35827307	Notification pod restarted after performing the upgrade from 23.2.2 to 23.3.0	The Notification pod restarted after performing the upgrade from SCP 23.2.2 to SCP 23.3.0.	2	22.4.4
35865799	SCP does not have an error log for DNS failures	SCP was missing specific cause and metric for DNS failure.	3	22.3.2
35909380	SCP is missing metrics for some error response and destination reselection.	SCP was missing metrics for some error responses and destination reselection.	3	23.2.2

Table 4-21 (Cont.) SCP 23.3.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35847868	Inter-SCP Routing SCP-P decodes scpPrefix from path incorrectly leaving an extra slash	The consumer SCP (SCP-C) added a forward slash at the end of the 3gpp-target-api-root header while sending the service request to producer SCP (SCP-P).	3	23.2.0

Table 4-22 SCP ATS 23.3.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35835777	SCP ATS : Oracle Internal LAB: SCP_22.3.0_Bug_Fixes feature is failing in regression run	The SCP_22.3.0_Bug_Fixes feature failed in regression run.	2	23.2.2
35847508	SCP ATS - Database tables cleanup issue post failure of a feature	The OutlierDetectionProducer_AUSF feature failed due to pod scaling issue and got the same pod scaling issue during the cleanup of the scenario.	2	23.2.2
35878434	SCP ATS - S3 of ModelD_based_Routing_implicit_notification feature is failing	Scenario 3 of the ModelD_based_Routing_implicit_notification feature failed in regression run due to metric mismatch.	3	23.3.0
35788053	SCP ATS New Features - S23 static config test case failed under SCP_Lci_Support.feature	Scenario was written with hardcoded timestamp values causing failure when that time expired.	3	22.4.2

Note:

Resolved bugs from 23.2.2 have been forward ported to Release 23.3.1.

Table 4-23 SCP 23.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35341610	Traffic failure(429 overload discard) was observed while running traffic at 231K TPS using 8vCPU as well as 12vCPU worker pod profiles	Traffic failure (429 overload discard) was observed while running traffic at 231K TPS using 8 vCPU and 12 vCPU worker pod profiles.	2	23.1.0
35389651	Worker pod restarts were observed intermittently while the traffic was running with the GL rate limit enabled with three SCPs.	SCP worker pod restarted intermittently while the traffic was running with the global rate limit enabled with three SCPs.	2	23.1.0

Table 4-23 (Cont.) SCP 23.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35593103	100K MPS SCP Traffic resulting in multiple restarts of all scp-worker pods	100K MPS SCP Traffic led to multiple restarts of all SCP Worker pods.	2	23.2.0
34608494	SCP worker pods have restarted while executing the 15K TPS with 2 Trigger points enabled	SCP worker pods restarted while running the 15K TPS with two trigger points enabled.	3	22.3.0
35122031	scp worker restarts noticed with 23.1.0 GA build while 30K MPS call-model with message-copy was in progress	In 23.1.0, an SCP worker pod restarted with 30K MPS message copy enabled towards OCNADD.	3	23.1.0
35189446	Overload discard with error observed after solution upgrade from 22.4.2 to 23.1.0	SCP discarded messages with errors after upgrade from 22.4.2 to 23.1.0.	3	23.1.0
35207808	54K MPS SCP message copy traffic test resulted in scp-worker restarts after 44 hours run	SCP worker pod restarted when tested with 54K MPS SCP message copy traffic after running for 44 hours.	3	23.1.0
35238177	scp-worker POD restarts when tested 7.2K MPS traffic per scp-worker POD with Message Copy	SCP worker pod restarted when tested with 7.2K MPS traffic per SCP worker pod with message copy.	3	23.1.0
35395598	Load value is not displayed under the SEPP NF profile in SEPP Registration.	The load value was not displayed under the SEPP NF profile in SEPP registration.	3	23.1.0
35347166	SCP Sending wrong domain name to DNS for querry	SCP sent the wrong domain name in DNS queries.	3	23.1.0
35363354	SCP not following algorithm for Priority within Locality for InterPLMN scenarios	SCP did not follow the algorithm for priority within locality for interPLMN scenarios.	3	22.3.3
35404678	SCP does not consider the response parameter in the Egress Host Preference in the case of InterPLMN routing	While running the InterPLMN routing, SCP did not consider the response parameter that was included in the Egress Host Preference.	3	23.1.0
35461260	SCP returns 500 Internal error In the case of an incorrect load metric value received from InterSCP	SCP returned a 500 internal error when an incorrect load metric value was received from InterSCP.	3	23.2.0
35531887	SCP upgrade from 23.1.0 to 23.2.0 failed due to notification-pre-upgrade pod being in ERROR status	SCP upgrade from 23.1.0 to 23.2.0 failed because the notification-pre-upgrade pod was in ERROR state.	3	23.1.0
35541182	Wrong cause is coming in Response code "400" BAD REQUEST while removing "type": "subject" in CCA header validation configuration.	Incorrect cause was observed in Response code "400" BAD REQUEST while removing "type": "subject" from the CCA header validation configuration.	3	23.2.0

Table 4-23 (Cont.) SCP 23.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35542359	SCP do not have pre-expiry alerts for SSL certificates	SCP did not have pre-expiry alerts for SSL certificates.	3	23.1.0
35545862	Console GUI SCP - Mismatch between API data and GUI for scp row in NF Rule Profile screen	SCP row in NF Rule Profile page could not be updated and saved as there was a mismatch between API data and CNC Console.	3	23.3.0
35602695	Egress Rate Limiting Not working as per the configuration done	Egress Rate Limiting was not working as per the configuration.	3	23.1.0
35629435	SCP GUI is showing 405-undefined error when we try to delete nf profile configuration instead of defined error	The SCP Console GUI displayed 405- undefined error on deleting the NF profile configuration instead of defined error.	3	23.2.0
35635743	Console GUI SCP - Mismatch of datatype in API and GUI Json in NF Rule Profile screen	In SCP Console GUI, mismatch of datatype in API and GUI Json was observed in NF Rule Profile page.	3	23.3.0
35686488	retryAfter & redirectUrl of PodOverloadActionPolicy marked M in Rest API Guide	retryAfter and redirectUrl parameters of `PodOverloadActionPolicy` were marked as mandatory in the *Oracle Communications Cloud Native Core, Service Communication Proxy REST Specification Guide*.	3	23.2.0
35691341	CNC Console SCP GUI - JSON data Model consists duplicate IDs which is accessibility issue at console	In SCP Console GUI, the presence of duplicate IDs in the JSON data model triggered accessibility issues.	3	23.2.0
35255824	SCP returns 500 Internal error when a mandatory parameter is missing while configuring egress host preference	SCP returned a 500 Internal Error when a mandatory parameter was missing while configuring the egress host preference.	4	23.1.0
35268879	SCP is not returned the details and cause with 400 error while configuring the missing mandatory parameter of server header configuration.	SCP did not return the problem details and returned a 400 error while configuring the missing mandatory parameter of the server header configuration.	4	23.1.0
35268980	SCP is returned 200 error while configuring invalid values of server header configuration.	SCP returned a 200 error while configuring invalid values for the server header configuration.	4	23.1.0
35276772	SCP is not returned the details and cause with 400 error while configuring the invalid message format of server header configuration.	SCP did not return the problem details and caused a 400 error while configuring the invalid message format of the server header configuration.	4	23.1.0

Table 4-23 (Cont.) SCP 23.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35281804	When User Agent Info parameters are not provided, the SCP console GUI is giving unidentified error.	When User Agent Info parameters were not provided while saving the configuration, the SCP Console GUI displayed an unidentified error.	4	23.1.0
35283493	SCP console GUI is giving 405:unidentified error, when IP End Points of an registered NF is deleted	SCP Console GUI displayed a 405 unidentified error when IP endpoints of a registered NF were deleted.	4	23.1.0
35301673	SCP GUI is giving unidentified error if Global Egress Rate Limit parameters are not provided	SCP Console GUI displayed an unidentified error if 'global egress rate limit parameters' were not provided.	4	23.1.0
35302303	Namespace is missing from the SCP dashboard metrics queries	Namespace was missing from the SCP dashboard metrics queries.	4	23.1.0
35326952	SCP GUI is responding with nfProfile of incorrect nfInstanceId, when we provide Query Parameters of correct nfInstanceId	When providing query parameters for the correct nfInstanceId, the SCP Console GUI responded with nfProfile for the incorrect nfInstanceId.	4	23.1.0
35377663	SCP returns 500 internal error in case of modifying InterSCP NF Profile from Console	SCP returned a 500 internal error when attempting to modify the InterSCP NF Profile from CNC Console.	4	23.1.0
35410691	SCP GUI is showing 401-undefined error when we provide Reroute Condition List parameter with invalid value	When an invalid value was provided for the Reroute Condition List parameter, SCP Console GUI displayed a 401-undefined error.	4	23.1.0
35443700	SCP Data Feeder - x-http2-stream-id is not received by SCP worker , but is present in INGRESS_REQUST header-list	SCP worker did not receive SCP data feeder-x-http2-stream-id, but it was present in the INGRESS_REQUST header list.	4	23.1.0
35443714	SCP Data Feeder - host header is not received by SCP worker , but is present in INGRESS_REQUST header-list	SCP worker did not receive SCP data feeder - host header, but the host header was added by SCP in the INGRESS_REQUST header list.	4	23.1.0
35449574	SCP displays the ocscp_nf_service_type parameter value as default rather than unknown in the ocscp_worker_fqdn_resolution_total metrics when sending notification messages from NRF	SCP displayed the '`ocscp_nf_service_type`' parameter value as default rather than unknown in the `ocscp_worker_fqdn_resolution_total` metric when sending notification messages from NRF.	4	23.2.0

Table 4-23 (Cont.) SCP 23.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35457962	SCP Dashboard needs correction for panel "NRF Proxy - Discovery Tx Requests Rate to NRF"	SCP dashboard for panel "NRF Proxy - Discovery Tx Requests Rate to NRF" did not show the correct results and returned an error.	4	23.2.0
35461249	SCP does not display the correct value for the parameter "ocscp_producer_instance_id " in ocscp_nf_load metrics in case of InterSCP	SCP did not display the correct value for the parameter "ocscp_producer_instance_id " in ocscp_nf_load metrics in the case of InterSCP.	4	23.2.0
35509612	SCP returns 400 undefined when "Enable Enhance Server Header Behaviour v1 and v2" options are enabled at the same time	SCP returned the 400 undefined error message when "Enable Enhance Server Header Behaviour v1 and v2" options were enabled at the same time.	4	23.2.0
35526886	SCP displays incorrect ocscp_error_group value for ocscp_metric_scp_generated _response_total metric	SCP displayed an incorrect ocscp_error_group value for the `ocscp_metric_scp_generated_response_total` metric.	4	23.2.0
35536359	IP-ADDRESS and URI-ID_APIROOT is configured twice while configuring preferred_validation_order in "tls_crt_san" of CCA header validation configuration.	IP-ADDRESS and URI-ID_APIROOT were configured twice while configuring preferred_validation_order in the "tls_crt_san" of CCA header validation configuration.	4	23.2.0
35537358	Wrong cause is coming in Response code "400" BAD REQUEST while configuring the custom cause Null in Error profile configuration.	Incorrect cause was observed in response code "400" BAD REQUEST while configuring the custom cause *Null* in Error profile configuration.	4	23.2.0
35588612	SCP GUI is showing 400-undefined error when we provide Access Token Validation Types parameter with invalid value || when we provide Access Token Validation Types parameter with supported value	SCP Console GUI displayed 400- undefined error when the Access Token Validation Type parameter was provided with invalid values.	4	23.2.0
35589089	SCP GUI is showing 400-undefined error when we provide Access Token Refresh Guard Time parameter with invalid value || when we provide Access Token Clean Up Post Expiry parameter with invalid value	SCP Console GUI displayed 400- undefined error when the Access Token Refresh Guard Time parameter was provided with invalid values.	4	23.2.0

Table 4-23 (Cont.) SCP 23.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35589131	SCP GUI is showing 400-undefined error when we provide Access Token Validity Guard Time parameter with invalid value || when we provide Access Token History Size parameter with invalid value	SCP Console GUI displayed 400- undefined error when the Access Token Validity Guard Time parameter was provided with invalid values.	4	23.2.0
35621044	SCP Console UI is not allowing to configure either INDIRECT_COM_WITH_DELEG_DISC or INDIRECT_COM_WITHOUT_DELEG_DISC values in SCP Access Token Capability parameter	SCP Console GUI did not allow to configure either INDIRECT_COM_WITH_DELEG_DISC or INDIRECT_COM_WITHOUT_DELEG_DISC values in the SCP Access Token Capability parameter.	4	23.2.0
35629306	In Console UI of SCP, oauth2_support feature flag is disabled but still able to configure the Access Token Validity Guard Time.	In the SCP Console GUI, even though oauth2_support feature parameter was disabled, the Access Token Validity Guard Time could still be configured.	4	23.2.0
35629412	In Console UI of SCP, Unable to configure either of DISCOVERY-HEADERS,CCA-HEADERS or USER-AGENT-HEADER in Requester Info	In SCP Console GUI, DISCOVERY-HEADERS,CCA-HEADERS or USER-AGENT-HEADER configuration in Requester Info were not getting configured.	4	23.2.0
35630019	In Console UI of SCP,400 response code is returned for all Feature Specific Config parameters when configured with alphabets.	In SCP Console GUI, 400 response code was returned for all Feature Specific Config parameters when configured with alphabets.	4	23.2.0
35636317	SCP GUI is showing 400-undefined error instead of defined error when we try provide “Please Select” to Actions	The SCP Console GUI displayed 400- undefined error instead of defined error when the Action option was set to "Please Select".	4	23.2.0
35641346	Access Token Granularity Configuration Rule name validation is missing.	Access Token Granularity Configuration Rule name validation was missing.	4	23.2.0
35643529	SCP returns an error while modifying Response Timeout and Total Transaction lifetime under Routing Options to higher values	SCP returned an error while modifying Response Timeout and Total Transaction lifetime to higher valuesunder Routing Options.	4	23.2.0
35675375	Transaction Success rate shows more than 100% in grafana board	Grafana dashboard displayed a transaction success rate of more than 100%.	4	23.2.1

Table 4-23 (Cont.) SCP 23.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35600630	SCP Installation Guide Subsection "Uninstalling SCP Using Helm" Has Command With Helm2 Syntax Not Helm3	The Helm command in the "Uninstalling SCP Using Helm" section was updated in the *Oracle Communications Cloud Native Core, Service Communication Proxy Installation, Upgrade, and Fault Recovery Guide*.	4	23.1.1
35668094	Documentation request for R15 and R16 SCP Configurable Routing Options in the SCP User Guide	The "Configurable Routing Options" section in the *Oracle Communications Cloud Native Core, Service Communication Proxy REST Specification Guide* was updated with R16 and R15 supported parameters.	4	23.2.0
35730451	PUT giving response as 204 during creation of STATIC SEPP Profile in SCP.	The PUT method returned 204 response while creating the STATIC SEPP Profile in SCP.	4	23.2.1
35748960	Upstream Service Time is missing in default grafana board	Upstream Service Time was missing on the default Grafana dashboard.	4	23.2.1
35687296	Legend is missing in Ingress request rate panel on default grafan board	Legend was missing in ingress request rate panel on the default Grafana dashboard.	4	23.2.1

Table 4-24 SCP ATS 23.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35229729	In ATS GUI test result is not displayed for few test cases	In ATS GUI, the test results were not displayed for a few test cases.	3	22.2.4
35469175	ATS fix for Kafka namespace issue	ATS framework for traffic feed feature test case Kafka name was appended in the SCP deployment namespace.	3	23.2.0

Note:

Resolved bugs from 23.2.2 have been forward ported to Release 23.3.0.

4.2.9 SEPP Resolved Bugs

Table 4-25 SEPP 23.3.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36153063	SEPP sending two "user-agent" headers, one with "Jetty/11.0.11" and another with "SEPP".	The two user-agent headers, "Jetty/11.0.11" and "SEPP", were generated by SEPP for patch/HB towards NRF. The extra header must be removed.	3	23.3.0
35890256	The SEPP Helm chart does not pass Helm Strict Linting	The SEPP Helm chart didn't pass the Helm Strict Linting. The key-duplicates error must be removed.	3	23.3.0
35767064	Rollback failed from 23.3.0 to lower versions with the error no ConfigMap with the name "rss-ratelimit-map" found.	SEPP Rollback failure was observed from 23.3.0 to earlier releases (23.1.x and 23.2.x) with the following error: no ConfigMap with the name "rss-ratelimit-map" found. This was a Helm issue where configmap was already present, but the Helm was considering it as not present, hence, it was resulting in an error.	3	23.3.0

Table 4-25 (Cont.) SEPP 23.3.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35767215	SEPP upgrade fails when performed for second time after performing rollback.	When upgrade was performed to SEPP Release 23.3.0 more than once, after performing a rollback, the upgrade failed with the following error: *UPGRADE FAILED: rendered manifests contain a resource that already exists. Unable to continue with update: ConfigMap "egress-ratelimit-map" in namespace "yash-upgrade" exists and cannot be imported into the current release: invalid ownership metadata; label validation error: missing key "app.kubernetes.io/managed-by": must be set to "Helm"; annotation validation error: missing key "meta.helm.sh/release-name": must be set to "ocsepp-release"; annotation validation error: missing key "meta.helm.sh/release-namespace": must be set to "yash-upgrade"* The example upgrade and rollback path: 23.1.3 (is upgraded to) 23.3.0 (rollback to) 23.1.3 (is upgraded to) 23.3.0: the upgrade failed here.	3	23.2.0

> **Note:**
>
> Resolved bugs from 23.1.x, 23.2.x, and 23.3.x have been forward ported to Release 23.3.2.

Table 4-26 SEPP 23.3.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35781995	SEPP-Install/Upgrade: Alternate-route image is not found in OCSEPP_23.3.0_CSAR _VZW package	Alternate-route image was not visible in OCSEPP_23.3.0_CSAR _VZW package. This was due to a new line tag missing at the end of the file.	2	23.3.0
35788676	PLMN IGW Information missing on Via header for cSEPP in TxResponse	The Via header for cSEPP in TxResponse was missing an accurate value for TxResponse on the home SEPP.	3	23.3.0
35829565	CONFIG_INVALID_NFI STANCE case keeps failing in ATS	"CONFIG_INVALID_NFI NSTANCE" failed at run.	3	23.3.0
35720372	SEPP 23.2.0 Fails TUH of 3ggp-sbi-routing-binding of N32_Ingress_Request	In SEPP 23.2.0, the Topology Recovery (TUH) operation failed for the Ingress request of the 3gpp-sbi-routing-binding header.	3	23.2.0
35830255	Remove duplicate pod information from CPU and Memory usage alert	SEPPPodCpuUsageAler t pod was appearing twice - pod and podname. This was due to the different label names for pod and podname.	4	23.3.0

Table 4-27 SEPP 23.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35629896	Unable to save/update network ID or service API validation lists in CAT1 & CAT2 after upgrading SEPP to 23.2.0	n SEPP 23.1.x release, the Default Service API Validation List (CAT1) and Default Network ID Validation List (CAT2) were present along with some other custom validation list(s). On upgrading to SEPP 23.2.0 release, the following error was observed while trying to save or update the validation lists that pre-existed in the setup. Error Code 400: Bad Request - 400 BAD_REQUEST "Invalid resourceURI / nsmf-pdusession/v1/pdu-sessions/ This 400 BAD_REQUEST error can be observed for multiple different resourceURIs, when reproducing the issue. This issue was observed while upgrading SEPP 23.1.0 and 23.1.3 to 23.2.0.	2	23.2.0
35608813	SEPP-FT-SCM-Cat3: nfStatusNotificationUri in notification subscription shall be updated	When the Cat-3 Previous Location Check feature was enabled, SEPP was sending subscription request to NRF for UDR profile changes. Since NRF is in different namespace, it is unable to resolve the ocsepp-pn32f-svc. FQDN in the nfStatusNotificationUri must be configured so it is reachable from NRF, when: • NRF is installed within the same cluster. • NRF is installed on a different cluster.	2	23.2.0
35476560	OCSEPP: Inconsistency observed in traffic while enabling message copy feature on SEPP.	The inconsistency was observed in the traffic while enabling the Message Copy feature in SEPP. While running the traffic with message copy enabled on PLMN Ingress Gateway, the traffic drop was observed in Grafana, but on aggregation, logs were seen only for SEPP traffic.	2	23.2.0
35080242	SEPP-PERF: High Memory & CPU usage on SEPP service with Topology Hiding, SCM(Cat1 & Cat2) with 2.5% rejection, Mediation & Ingress rate limit, Over Load features enabled during SEPP performance run	The memory usage was high for SEPP service with Topology Hiding, SCM (Cat-1 and Cat-2) with 2.5% rejection, Mediation, Ingress rate limit, and Overload features enabled during the SEPP performance run.	2	22.4.0

Table 4-27 (Cont.) SEPP 23.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35661898	pn32f and cn32f taking restarts at low tps if the uri is unique for the same API	While running the traffic at low TPS (10) with unique IMSI in an API (For example: /nudm-sdm/v2/imsi-{{.imsi}}/sdm-subscriptions), cn32f and pn32f CPU go to 100% and both the pods fail.	2	23.2.0
35639082	SEPP-FT-SCM-Cat3: SEPP sending GET authentication-status request to UDR with incoming request body and headers	SEPP copied the payload and headers while sending the GET request to the UDR.	3	23.2.0
35600048	SEPP-FT-SCM: IMSI regex needs to be changed to permit 15 digits only instead of 15 or 16	For the Cat-3 Previous Location Check feature, the allowed IMSI length was 15 or 16, whereas the correct value was 15. Hence, the length of all regex for UE ID should be 15 and the custom yaml should be updated for the feature section with regex length 15.	3	23.2.0
35566226	SEPP-FT-Cat0: Message validation API deleted from message schema configuration cannot be re-added	Message validation API once deleted from message schema configuration could not be added again.	3	23.2.0
35208390	SEPP-Upgrade: cn32f and pn32f pods restart observed during cndb rollback from 23.1.0 to 22.4.0	The cn32f and pn32f pods restarted during cnDBTier rollback from 23.1.0 to 22.4.0. As a result, the traffic was impacted.	3	23.1.0
35488522	isEnabled=FALSE functionality is not working as expected	In Remote SEPP Set, isEnabled functionality did not work as expected and Remote SEPP set could not be deleted when isEnabled was set to false.	3	23.2.0
35629371	SEPP-FT-SCM-Cat3: plmn-id shall be updated to plmnId in Cat3 - Body IE - Serving Network ID Body IE	In CNC Console, the plmn-id must be updated as plmnId in the Cat 3 - Previous Location Check feature.	3	23.2.0
35614264	SEPP-FT-SCM-Cat3: SEPP creates separate subscription for each pn32f-svc pod replica	SEPP created separate subscription for each pn32f-svc pod replica. Example: • `pn32f-svc replica= 1; subscription created on NRF = 1` • `pn32f-svc replica = 10; subscription created on NRF = 10` The expected behavior is there must be only one subscription, regardless of the number of pn32f-svc pod replicas.	3	23.2.0
35659123	SEPP-FT: podname blank in SEPPPodMemoryUsageAlert and SEPPPodCpuUsageAlert	The podname was blank in `SEPPPodMemoryUsageAlert` and `SEPPPodCpuUsageAlert`.	4	23.2.0

Table 4-27 (Cont.) SEPP 23.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35649111	SEPP-FT-Cat0: Remove duplicate attributes from alerts	The alerts `SEPPN32fMessageValidationOnHeaderFailureCriticalAlert`, `SEPPN32fMessageValidationOnHeaderFailureMajorAlert`, and `SEPPN32fMessageValidationOnHeaderFailureMinorAlert` have the duplicate parameters, podname and pod and app and appname.	4	23.2.0
35615394	SEPP-FT-SCM-Cat3: nf_instance_id dimension needs to be updated for metric ocsepp_previous_location_validation_success_total	The dimension nf_instance_id must be updated to nfinstanceid in the metric `ocsepp_previous_location_validation_success_total`.	4	23.2.0
35626673	SEPP-FT-Cat0: NFinstanceid is not displayed for alert SEPPN32fMessageValidationOnHeaderFailureCriticalAlert	The parameter `NFinstanceid` is not displayed for alert `SEPPN32fMessageValidationOnHeaderFailureCriticalAlert`.	4	23.2.0
35440232	SEPP Rollback : Some of the SEPP table data gets replicated after rollback	When a rollback is performed from 23.2.0 to 23.1.x, 22.4.x, and 22.3.x, some of the table data was replicated. This data must be either removed or updated during the upgrade.	3	23.2.0
35322202	SEPP-FT-SCM: Target-plmn-list shall be changed to PSEPP in default header list	For Cat 2 - Network ID Validation feature, in CNC Console, under the header, search for nnrf-disc, the header name available will be target-plmn-list. In the default configuration, the associated SEPP type for this header is C-SEPP, whereas it must be P-SEPP.	3	23.1.1
35292215	SEPP-FT: Details to all parameter is not displayed for alerts SEPPN32fNetworkIDValidationHeaderFailureAlert and SEPPN32fNetworkIDValidationBodyIEFailureAlert	The values of `nfinstanceid` and `requestPath` parameters were not displayed in the following alerts: • `SEPPN32fNetworkIDValidationHeaderFailureAlert` • `SEPPN32fNetworkIDValidationBodyIEFailureAlert`	3	23.1.0
35240823	SEPP-FT-SCM: Incorrect error code displayed instead of configured error code when done for 406.	While configuring the Cat-1 feature, if the Allowed List was configured for error code 406, incorrect error code was displayed.	3	23.1.0
35239997	SEPP-FT: SEPP not forwarding 308 status code to consumer	For the following scenarios: • Model-B configuration on both C-SEPP and P-SEPP • Producer responding with 308 and location header, the consumer should receive 308 and location header in the response instead of 504 Gateway Timeout.	3	23.1.0

Table 4-27 (Cont.) SEPP 23.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35222478	SEPP-FT-SCM: REST API to delete a specific rule from an existing list not working	The delete operation for deleting a specific rule from an existing rule list in the REST API Network ID Validation Allowedlist did not work.	3	23.1.0
35211643	SEPP Upgrade & 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 resulted in restarting the SEPP pods.	3	23.1.0
34976111	SEPP-FT-SCM: Custom yaml should provide parameters to allow/not allow internal headers	Internal headers were displayed in the response and request. The `ocsepp_customvalues_23.2.0.yaml` file must have the option to disable them as internal headers should not be displayed.	3	22.4.0
34953499	SEPP-FT-HostedSEPP: HostedSEPP adding two via header in request and response flow	Hosted SEPP added two *via headers* in request and response.	3	22.4.0
34760842	RH SEPP doesn't set a proper authorities in established N32 context with 3GppSbiTargetApiRootSupported " set to false	The following scenario was observed while sending the message from the Consumer NF to target NF through Roaming Hub: • Consumer SEPP sent a signaling request with 3gpp-sbi-target-apiroot HTTP header included in Roaming Hub (RH) SEPP that must be routed to target SEPP. • The RH SEPP handshake status shows that the N32 context established with target SEPP has 3GppSbiTargetApiRootSupported set to false. • The outgoing request from RH SEPP to target SEPP has no 3gpp-sbi-target-apiroot but the authority is replaced by the target SEPP identity and not with the identity found in the 3gpp-sbi-target-apiroot from the incoming request.	3	22.3.0
35594057	SEPP-FT-Cat0: NFinstanceid is not displayed for alert SEPPN32fMessageValidationOnBodyFailureCriticalAlert	The NFinstanceid was not displayed for alert `SEPPN32fMessageValidationOnBodyFailureCriticalAlert`.	4	23.2.0

Table 4-27 (Cont.) SEPP 23.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35590178	SEPP-FT-Cat0: Corrections needed for Cat0 metrics in SEPP user guide	The metric name was corrected from `ocsepp_message_validation_on_body_failure` to `ocsepp_message_validation_on_body_failure_total`. In the metric `ocsepp_message_validation_applied_total`, the dimension must be updated from `request_path` to `requestPath` in the *Oracle Communications Cloud Native Core, Security Edge Protection Proxy User Guide*.	4	23.2.0
35588838	SEPP-FT: ID to be returned for configurations being done for features: SOR, Cat0 and Cat3	The ID should be returned from the Database for the features SOR, Cat-0, and Cat-3 whenever any POST configuration is created.	4	23.2.0
35578368	SEPP-FT-SCM-Cat3: Response code for duplicate "Header --> UE ID" and "Body --> Service NetworkID" config are different	The response code for the duplicate header and duplicate body was different. • SEPP responded with the error code 400 while creating a duplicate Header in UE ID record. • SEPP responded with error code 406 while creating a duplicate Body in Serving Network Id. Both the error codes must be either 400 or 406.	4	23.2.0
35577807	SEPP-FT-SCM-Cat3: Response status code and code in response body shall be same	In the Cat -3 feature trigger rule list, the response status code and code in response body were not same. Example: To delete a non-existing Cat3 trigger rule list: `{"timestamp":"2023-07-07T05:45:10.376+00:00","status":400,"error":"Bad Request","message":"404 NOT_FOUND \"Previous Location Check Trigger List is missing in DB\"","path":"/sepp-configuration/v1/security-counter-measure/previous-locatio n-validation/auto-dummy"}` The expected status code response was 404 instead of 400.	4	23.2.0
35574882	SEPP-FT-Cat0: Correct the response Status for message validation list create and update request	The user received a wrong response code while creating or updating a message validation list.	4	23.2.0

Table 4-27 (Cont.) SEPP 23.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35570369	SEPP 23.2.0 Rest API for Mediation System Option has incorrect example	An incorrect example for Mediation System Option in the *Oracle Communications Cloud Native Core, Security Edge Protection Proxy REST API Guide* was added.	4	23.2.0
35568968	SEPP-FT-Cat0: Response code needs to be corrected when user tries to delete message validation list associated with remote SEPP set	The user received a wrong response code while deleting the trigger rule list associated to Remote SEPP Set.	4	23.2.0
35566252	SEPP-FT-Cat0: Misleading error needs to be corrected, incase invalid message schema is entered by user	When the user was updating the Message Schema (JSON) with invalid format, a misleading error code was displayed: "`Error Code: 400 - Bad Request - Exception occurred while saving configuration in database`."	4	23.2.0
35502633	SEPP-FT: Section 6.4 Cleaning up Databases; list of tables need to be updated	In *Oracle Communications Cloud Native Core, Security Edge Protection Proxy Installation, Upgrade, and Fault Recovery Guide*, only 52 tables were listed in the Cleaning up Database section instead of 57.	4	23.2.0
35463134	SEPP-FT: n32cHandshakePlmnIdListSend shall be updated to "true" in custom yaml	In `ocsepp_customvalues_23.2.0.yaml` file, the `n32cHandshakePlmnIdListSend` was set to false for Remote SEPP Exchange Capability request, but in *Oracle Communications Cloud Native Core, Security Edge Protection Proxy Installation, Upgrade, and Fault Recovery Guide*, `n32cHandshakePlmnIdListSend` value was set to true.	4	23.2.0
35377315	SEPP-FT: Data missing for attributes source and nfinstanceid for SEPPPn32fSORFailureAlert	For the alerts `SEPPPn32fSORFailureAlertPercent30to40`, `SEPPPn32fSORFailureAlertPercent40to50`, and `SEPPPn32fSORFailureAlertPercentAbove50`, the source and `nfinstanceid` parameters did not display any data.	4	23.1.1
35363038	SEPP-SOR-FT: SEPPPn32fSORTimeoutFailureAlert has blank source and nfinstanceid	In `SEPPPn32fSORTimeoutFailureAlert`, the data was missed in the source and `nfinstanceid` fields.	4	23.1.1

Table 4-27 (Cont.) SEPP 23.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35354225	SEPP-SOR-FT: sorRemoteSepp should be changed in RSS payload	In the Payload for Remote SEPP Set, the parameter name `sorRemoteSepp` must be corrected to reflect SoR Trigger Rule List Name.	4	23.1.1
35349458	SEPP-SOR-FT: Response code needs correction when user tries to delete trigger rule list associated to RSS	When the user tried to delete trigger rule list associated to RSS, incorrect response code was displayed.	4	23.1.1
35348842	SEPP-FT: On adding a new header/body config for Cat2, ID should be returned	On adding a new header or body configuration for Cat 2 - Network ID Validation feature, the ID must be returned.	4	23.1.1
35292187	SEPP-FT: Correct the metric names ocsepp_network_id_validation_body_failure_total and ocsepp_network_id_validation_header_failure_total	The following metric names must be corrected in the *Oracle Communications Cloud Native Core, Security Edge Protection Proxy User Guide*: `ocsepp_network_id_validation_body_failure` must be corrected to `ocsepp_network_id_validation_body_failure_total`. `ocsepp_network_id_validation_header_failure` must be corrected to `ocsepp_network_id_validation_header_failure_total`.	4	23.1.0
35248911	SEPP-FT-SCM: Response code needs to be corrected when user tries to delete Network ID validation list associated with remote SEPP set	When the user was deleting the Network ID validation list associated with RemoteSEPP Set, the Error Code 401 was displayed.	4	23.1.0
35173775	SEPP not showing producer-fqdn(in metadata) of end producer instead using it from YAML in message-copy	SEPP did not display the producer-fqdn of the end producer. It instead displayed the value from the `ocsepp_customvalues_<version>.yaml` in Message Copy feature. The producer FQDN was as per the SEPP yaml, but the value should be derived from incoming 3gpp-sbi-target-apiroot. To avoid the disparity, SEPP should avoid populating these particular values from the `ocsepp_customvalues_<version>.yaml` file.	4	23.1.0

Table 4-27 (Cont.) SEPP 23.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35677428	SEPP Regression pipeline requires modification to plmnIdList for Procedure 3.7.4.7 of ATS User Guide	The documentation has to be updated for setting up the test case for success as in some cases, SEPP regression pipeline was failing. The issue was observed in the following scenarios: • Message forward to Remote SEPP when mediation, topology, SCM, and network Id Validation were enabled. • At local SEPP mediation and Remote SEPP mediation, query parameters were modified. • Topology was performing operations on the same query parameters and network Id validation was validating PLMN of supi in query parameters.	4	23.2.0
35514700	SEPP-FT: client_type parameter to be corrected for metric ocsepp_cn32f_jetty_request_stat_metrics_total in user guide	In the `ocsepp_cn32f_jetty_request_stat_metrics_total`, the parameter name must be corrected from `clientType to client_type` in *Oracle Communications Cloud Native Core, Security Edge Protection Proxy User Guide*.	4	23.2.0
35173724	SEPP not populating consumer-id and consumer-fqdn from user-agent in case of EGW message copy	The consumer-id and consumer-fqdnconsumer-fqdn should be fetched from the User Agent if it is present in SEPP. However, SEPP did not populate the consumer-id and consumer-fqdn from User Agent in case of Egress Gateway Message Copy feature.	4	23.1.0
35630061	SEPP-ATS: SEPP(Mediation and Coherence) and CNDB resource profile not given at SEPP ATS documents for sepp & cndb installation	The Mediation and Coherence resource profiles were not documented in the *Oracle Communications Cloud Native Core, Automated Testing Suite Guide*.	4	23.2.0

Note:

Resolved bugs from 23.1.0, 23.1.1, 23.1.2, 23.1.3, 23.2.0, and 23.2.1 have been forward ported to Release 23.3.0.

4.2.10 UDR Resolved Bugs

Table 4-28 UDR 23.3.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36179774	Service account creation issue for STUB installation in SLF 23.3.1	STUB installation was creating a service account even though the create value was set to false.	2	23.3.1
36200825	SLF ATS test case Subscriber export failure	Multiple test scenarios failed for subscriber export tool.	3	23.3.1

Table 4-29 UDR 23.3.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35800164	UDR - After doing Inservice Upgrade of UDR from 23.1.2 to 23.3.0 we are observing complete failure in Sh traffic	When performing in-service upgrade of UDR from 23.1.2 to 23.3.0, there was failure in Sh traffic with diameter result code of 3002.	2	23.3.0
35854659	UDR Upgrade 23.2 to 23.0 - Diameter Peers are upgraded with 'responseOnly' flag set to true	When upgrading UDR 23.2.0 to 23.3.0, diameter peers were upgraded with responseOnly flag set to true.	2	23.3.0
35912845	UDR is rejecting PUR for Quota with 5105 ERROR	UDR was rejecting Profile Update Request (PUR) for quota with 5105 ERROR.	2	23.3.0
35883286	SLF - In CNCC GUI NF scoring feature is not visible for SLF mode	NF scoring feature was not visible for SLF mode in the CNC Console.	2	23.3.0
35409689	PROVGW- In Provgw service configuration Retry error codes are not editable through CNCC	Retry error codes were not editable using CNC Console for Provision Gateway service configuration.	3	23.3.0
35762439	Retrieving quota with name and cid failing on VSA APIs where subscriber has mk1 and 4g quota	Retrieving quota with name and CID failed on VSA APIs when subscriber had mk1 and 4G quota.	3	23.3.0
35840439	Diam GW initiates CER eventhough responseOnly flag set to false	Diameter Gateway was initiating Connection Establishment Request (CER) even if the responseOnly flag was set to false.	3	23.3.0

Table 4-29 (Cont.) UDR 23.3.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35878216	UDR diameter PUR traffic is failing with error code 5012 when etag flag is false	When Entity Tag (ETag) flag was set to false, UDR diameter Profile Update Request (PUR) traffic failed with error code 5012.	3	23.3.0
35907958	UDR ATS 23.3 - New Features pipeline failing with Multiple Errors	New Features pipeline was failing with multiple errors for UDR ATS.	3	23.3.0
35917088	SLF-ATS 23.3.0 - Lab Performance pipeline issue in Declarative: Post Actions	Lab Performance pipeline issue was found in SLF-ATS 23.3.0.	3	23.3.0
35762518	SLF-ATS 23.3.0 - Lab Performance pipeline issue in Declarative: Post Actions	Lab performance pipeline issue was found in SLF-ATS 23.3.0.	3	23.3.0
35518071	UDR Few parameters from umdata related to Quota are not present in sm-data schema validation	Parameters from umdata related to quota were missing in sm-data schema validation.	4	23.3.0

Table 4-30 UDR 23.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35508533	UDR is not sending notification to PCF for subscriber deletion during active GX session	UDR did not send notification to Policy Control Function (PCF) when subscriber was deleted during an active session.	2	23.2.0
35410952	PUR update of state data is not generating notification when subscription is created for SM-DATA	Notification was not generated when Sh-Profile Update Request (PUR) request was sent to update the state data.	3	23.2.0
35243448	DNN Validation is missing while provisioning the SM-DATA	Deep Neural Networks (DNN) validation was missing as per 3GPP specification when provisioning the sm-data.	3	23.1.0
35065447	DB Records are not sync properly after network replication recovery	The database records were incorrectly synchronized when the network replication recovered after the replication outage.	3	22.4.0

Table 4-30 (Cont.) UDR 23.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35402560	Provgw disable jaegerTracingEnabled to stop Jaeger log collection	There was a requirement to stop log collection in Provisioning Gateway by disabling `jaegerTracingEnabled` parameter.	3	23.1.1
35616271	Failure of regression test ProvGw_SegDown_Success_04	The regression test failed as the Provisioning Gateway and Egress Gateway sent the request only to OCUDR Ingress Provisioning Gateway.	3	23.1.0
35361100	SLF 23.1.1 disable jaegerTracingEnabled to stop Jaeger log collection	There was a requirement to disable `jaegerTracingEnabled` parameter to stop log collection for jaeger in performance pod and config server pod.	3	23.1.1
35504059	CNCC not able to retrieve UDR information for GUI after upgrade to 22.4.0	CNC Console displayed 404 Not_Found error when accessing the UDR data after upgrading the CNC Console from 22.3.0 to 22.4.0.	3	22.4.2
35621246	Etag data type is integer instead of String in POST Notification message	Entity Tag (Etag) data type must be string instead of integer in POST notification message.	3	23.2.0
35540774	"RollBack" Option is missing in "Schema Management Data" UI Page	The Rollback option was missing in the CNC Console Schema Management Data page.	3	23.2.0
35540738	Unable to delete schema from Console, observing "Invalid URI" error	The schema was not deleted in the CNC Console Schema Management Data page. As a result, CNC Console displayed *400 Invalid URI* sent from client.	3	23.2.0
35457532	UDR VSA delete method is giving expected response.	Vendor Specific Attribute (VSA) was not getting deleted and returned 404 data field does not exist error.	3	23.2.0
35455140	SLF- Not able to change Control Shutdown operational state through CNCC GUI	The control shutdown operational state could not be modified through CNC Console.	3	23.2.0

Table 4-30 (Cont.) UDR 23.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35420398	While configuring the export tool parameter with rest api, the command is expecting the "remote path" parameter as mandatory attribute always	When using REST API to configure the export tool, the remote path parameter is a mandatory attribute in the command.	3	23.2.0
35520600	Alerts are not being generated in Prometheus for non-HA Prom	Alerts were not generated in Prometheus and Alert-Manager Graphical User Interface (GUI) for non-High Availability (HA) Prometheus.	3	23.1.1
35561766	Cndbtier upgrade failed from 22.4.1-23.2.0 with SLF Package DB yaml	cnDBTier upgrade failed from 22.4.1 to 23.2.0 because the heartbeatintervaldbdb parameter was not present in ocudr_slf_37msub_dbtier_23.2.0_custom_values_23.2.0 file.	3	23.2.0
35425766	EIR 23.1.0 - Log file created on SFTP server should contains underscore	The log file created on Secure File Transfer Protocol (SFTP) server contained hyphen instead of underscore before the file name.	4	23.1.0
35518071	UDR Few parameters from umdata related to Quota are not present in sm-data schema validation	In the sm-data schema, parameters related to 4G quota were missing from umdata schema validation.	4	23.2.0
35415161	UDR Unexpected log printing in diam-gateway and dr-provservices	Unexpected logs were printed repeatedly in Diameter Gateway and dr-provservices.	4	23.2.0

Note:

Resolved bugs from 23.1.2 have been forward ported to Release 23.3.0.

4.2.11 Common Services Resolved Bugs

4.2.11.1 Egress Gateway Resolved Bugs

Release 23.3.x

Table 4-31 Egress Gateway 23.3.x Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release	Fixed in Release
35727464	[NRF-APIGW]Egress Gateway is returning unknown host execption during SLFLookup with peermonitoring enabled	When peer monitoring feature was enabled and SLF-discovery request was sent to NRF, Egress Gateway returned 503 Service-Unavailable response and unknownHostExceptio n was observed at Egress Gateway.	2	23.3.1	23.3.4
35574383	[SEPP-APIGW] DNS SRV Support- Cache does not refresh once TTL in DNS SRV Entry expires. Forced restart of svc is required for changes to reflect	Cache did not refresh when TTL in DNS SRV Entry expired. svc (plmn egw and alt svc) was forcibly restarted to refresh the cache.	2	23.2.3	23.3.2
35336043	[PCF-APIGW] EGW not able to fetch config-map details saying - "config-map with name : <config-map-name> not present in namespace : <ns> "	[PCF-APIGW] EGW was unable to fetch config-map details stating: "`config-map with name : <config-map-name> not present in namespace : <ns>` ".	2	22.4.4	23.3.1
35495609	[PCF-APIGW] SM PCF responding with "Null" cause values	[PCF-APIGW] SM PCF responded with *"Null"* cause values.	3	22.3.3	23.3.1
35412487	[PCF-APIGW] [CNCESPOL-1497]_Vz w pre prod- AM PCF-EGW SCP comminucation issue	When Webscale was upgraded, AM-PCF was scaled down. When the system was scaled up after MW, 500 error was observed at PCF-EGW.	4	22.4.3	23.3.1
35434597	[NRF-APIGW] EGW is performing peermonitoring incorrectly and sending the request to unhealthy peer	[NRF-APIGW] EGW incorrectly performed peer monitoring and sent the request to unhealthy peers.	2	23.2.4	23.3.0

Table 4-31 (Cont.) Egress Gateway 23.3.x Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release	Fixed in Release
35419929	[SEPP-APIGW] Null Pointer Exception when TLS handshake failure happens	[SEPP-APIGW] Null Pointer Exception was observed when TLS handshake failure occurred.	4	23.1.3	23.2.4
35109371	[PCF-APIGW] Egress gateway is reporting IllegalReferenceCount Exception in every 2sec.	[PCF-APIGW] Egress Gateway reported IllegalReferenceCount Exception every 2 seconds.	3	23.1.3	23.3.0
35391273	[NRF-APIGW] SCP Monitoring egw api is not returning the correct status of configured peer	[NRF-APIGW] SCP Monitoring egw api did not return the correct status of configured peer.	2	23.2.2	23.3.0
35391415	[NRF-APIGW] SCP Monitoring oc_egressgateway_peer_health_status is not getting pegged correctly	[NRF-APIGW] SCP Monitoring oc_egressgateway_peer_health_status was not pegged correctly.	2	23.2.2	23.2.3

4.2.11.2 Ingress Gateway Resolved Bugs

Release 23.3.x

Table 4-32 Ingress Gateway 23.3.x Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release	Fixed in Release
35723545	OC-XFCC-DNS header not received from Gateway error	The OC-XFCC-DNS header was not received in Gateway error, resulting in pipeline failure for the scenarios where DNS was missing.	2	23.3.1	23.3.3
35722786	Control shutdown feature not working - IGW not rejecting the requests	After the Controlled Shutdown feature was enabled and set to COMPLETE_SHUTDOWN, requests were not rejected.	2	23.3.1	23.3.3
35672556	[NRF-APIGW] OC-XFCC-DNS header not received from Gateway error	The OC-XFCC-DNS header was not received in Gateway error, resulting in Feature Test failure in pipeline.	2	23.3.0	23.3.2

Table 4-32 (Cont.) Ingress Gateway 23.3.x Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release	Fixed in Release
35667118	[NEF-APIGW] Repeated Jaeger Trace Ids	While doing the Open Telemetry tracing test in NEF, the same trace IDs were generated in Ingress Gateway after every fourth request.	3	23.3.0	23.3.1
34930585	[SEPP-APIGW] Gateway sending "5g-sbi-message" with a New line and Tabs (\n & \t) on Kafka	5g-sbi-message was sent with special characters, such as new line, Tabs "\", "\n", "\t", and so on, to Kafka for both call flows and Erroneous Scenarios when Message Copy was enabled on all gateways.	4	22.4.1	23.3.1
35523042	[NRF-APIGW]: IGW closing TCP connections within 2 min	Ingress Gateway was closing TCP connections every 2 minutes.	2	23.1.4	23.3.0
35178811	[BSF] [Overload] http Overload discards traffic is not shown in "ocbsf_oc_ingressgateway_http_responses_total" metric	[BSF] [Overload] http Overload discards traffic is not shown in "`ocbsf_oc_ingressgateway_http_responses_total" metric`	3	22.4.2	23.3.0

4.2.11.3 NRF-Client Resolved Bugs

Table 4-33 NRF-Client 23.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35745511	nrf-client-nfmanagement service crashing with enablePDBSupport flag enabled and replicas set as 2	The pods crased with error "`Invalid data present in the secret [...] looking for keys[...]`", when enablePDBsupport is enabled and replicas set as 2 for nrf-client-nfmanagement service.	2	23.3.1

4.2.11.4 ATS Resolved Bugs

Table 4-34 ATS 23.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35647154	Log seems to point issue in Parallel Execution when the problem is due to Parameterization	When there was an issue with parameterization, the logs seemed to point to a problem with parallel_info_file, due to which a hook_error was raised.	3	23.2.0
35647023	Applogs have 3rdRerun, 4thRerun and 5thRerun related logs	After enabling applogs from Jenkins, it was observed that in the applogs there are logs related to the 3rd, 4th, and 5th reruns.	3	23.2.0
35623943	Development server warning received in ATS pod along with Network unreachable exception	After deploying ATS for Data Director 23.2.0, the warning was observed in the logs of the ATS pod.	3	23.2.0
35352880	Parallel execution: before_stage and after_stage hooks to run only if the specific stage related cases are chosen	It was observed that when a certain test case was executed in stage 2, the before_stage and after_stage of stage 1 and stage 3 were also running.	3	23.2.0

4.3 Known Bug List

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

4.3.1 CDCS Known Bugs

CDCS Release 23.3.1

Table 4-35 CDCS 23.3.1 Known Bugs

Bug Number	Title	Description	Severity	Found in Release	Customer Impact
35925777	Create Production/Staging Site fails when tried with Bastion Host user other than default	Installation of CNE using CDCS fails when the installation is performed using a username other than cloud-user on the Bastion Host.	3	23.2.0	Users will be limited to use only one user while deploying CNE.

CDCS Release 23.3.0

Table 4-36 CDCS 23.3.0 Known Bugs

Bug Number	Title	Description	Severity	Found in Release	Customer Impact
35372347	Create Production/Staging Site fails when non-default Bastion Host user specified	CNE installation using CDCS fails when users attempt to install CNE using a username other than cloud-user on the Bastion Host.	3	23.2.0	Users can use only one user while deploying CNE.
35820090	Remove Worker Node pipeline is not waiting for pods to come up	The Remove OCCNE Worker Node pipeline is failing.	3	23.2.0	The hosts.ini file does not get updated after the worker node is removed due to pipeline failure before performing the operation.

4.3.2 CNC Console Known Bugs

CNC Console 23.3.2

There are no known bugs in this release.

CNC Console 23.3.1

There are no known bugs in this release.

CNC Console 23.3.0

There are no known bugs in this release.

4.3.3 CNE Known Bugs

CNE 23.3.5 Known Bugs

There no new known bugs in this release. For existing known bugs, see CNE 23.3.4 Known Bugs.

Table 4-37 CNE 23.3.4 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36125787	OCCNE 23.2.5 Issue in adding new lbvm in vCNE	While adding a new pair of LBVMs to vCNE in an OpenStack environment, the `lbCtrlData.json` file populated by `./scripts/addPeerAddrPools.py` is incorrect.	The output of the script corrupts the data on the lbCtrlData.json file by changing the SubnetId and Network ID of the existing PeerAddressPools. This leads to misconfiguration of the systems and loss of connection. **Workaround:** There is no workaround for this bug.	2	23.2.5

Table 4-37 (Cont.) CNE 23.3.4 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35426047	removeWorkerNode.py not targeting node (Openstack)	While running the automated script to remove a Kubernetes worker node, the script does not target the specific node (given as an argument) while calling terraform. This causes terraform to always delete the last worker node from its list, instead of the targeted node.	Running the procedure to remove a Kubernetes worker node using `removeWorkerNode.py` for any node other than the last one causes terraform to delete the wrong node. However, the correct node gets deleted from the Kubernetes node list and LB controller configuration. This leaves the cluster in an unhealthy state in which neither of the affected nodes is correctly removed. **Workaround**: Do not use the Removing a Worker Node script to remove a worker node. If the procedure is already run and the cluster is in an unhealthy state, perform the following steps: • Manually remove the correct targeted node using terraform. • Manually remove the other impacted node (last in the list) from	3	23.2.0

Table 4-37 (Cont.) CNE 23.3.4 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
			the LB Controller and Kubernetes.		

CNE 23.3.3 Known Bugs

There no new known bugs in this release. For existing known bugs, see CNE 23.3.2 Known Bugs.

Table 4-38 CNE 23.3.2 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35527486	SPAD_POLICY: rook-ceph pods are getting restarted	Three Custom Resource Definitions (CRDs) found in `k8s_install/upgrade_/templates/`, have `v1beta1` version and are not getting created. As a result, the `csi-snapshotter` container of the `csi-cephfsplugin-provisioner` pod are encountering errors while taking snapshots.	The pods get restarted constantly which could affect the availability of data. **Workaround**: Change the version of CRD YAML files from `v1beta1` to v1 and increase the memory on these pods.	2	22.4.3

Table 4-38 (Cont.) CNE 23.3.2 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35369547	Target index not getting deleted as part of ILM	When a targeted index is deleted, it gets recreated automatically. This creates an issue as the user has to continuously monitor the indexes and manually manage the indexes on CNE. The steps to manage indexes are not functioning as expected.	OpenSearch ILM policies don't transition between hot, warm, and delete states. This bug is addressed partially in 23.2.0, where the state gets transitioned from hot to warm. However, the issue still persists when transitioning to the delete state. **Workaround**: • If you are installing 23.1.1, configure the index management policy for OpenSearch Dashboard after the installation. For procedure, see the "*Verifying and Configuring Common Services*" section in 23.1.1 *Oracle Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide*. • If you are upgrading from 23.1.x	2	23.1.1

Table 4-38 (Cont.) CNE 23.3.2 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
			to 23.2.0, configure the index management policy for OpenSearch Dashboard before performing an upgrade. For procedure, see the "*Configuring Index Management Policy for OpenSearch Dashboard*" section in 23.2.0 *Oracle Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide*.		

Table 4-38 (Cont.) CNE 23.3.2 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35426047	removeWorkerNode.py not targeting node (Openstack)	While running the automated script to remove a Kubernetes worker node, the script does not target the specific node (given as an argument) while calling terraform. This causes terraform to always delete the last worker node from its list, instead of the targeted node.	Running the procedure for any node other than the last one causes terraform to delete the wrong node. However, the correct node gets deleted from the Kubernetes node list and LB controller configuration. This leaves the cluster in an unhealthy state in which neither of the affected nodes is correctly removed. **Workaround**: Do not use the Removing a Worker Node script to remove a worker node. If the procedure is already run and the cluster is in an unhealthy state, perform the following steps: • Manually remove the correct targeted node using terraform. • Manually remove the other impacted node (last in the list) from the LB Controller and Kubernetes.	3	23.2.0

Table 4-39 CNE 23.3.1 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35527486	SPAD_POLICY: rook-ceph pods are getting restarted	Three Custom Resource Definitions (CRDs) found in `k8s_install/upgrade_/templates/`, have `v1beta1` version and are not getting created. As a result, the `csi-snapshotter` container of the `csi-cephfsplugin-provisioner` pod are encountering errors while taking snapshots.	The pods get restarted constantly which could affect the availability of data. **Workaround**: Change the version of CRD YAML files from `v1beta1` to v1 and increase the memory on these pods.	2	22.4.3

Table 4-39 (Cont.) CNE 23.3.1 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35369547	Target index not getting deleted as part of ILM	When a targeted index is deleted, it gets recreated automatically. This creates an issue as the user has to continuously monitor the indexes and manually manage the indexes on CNE. The steps to manage indexes are not functioning as expected.	OpenSearch ILM policies don't transition between hot, warm, and delete states. This bug is addressed partially in 23.2.0, where the state gets transitioned from hot to warm. However, the issue still persists when transitioning to the delete state. **Workaround**: • If you are installing 23.1.1, configure the index management policy for OpenSearch Dashboard after the installation. For procedure, see the "*Verifying and Configuring Common Services*" section in 23.1.1 *Oracle Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide*. • If you are upgrading from 23.1.x	2	23.1.1

Table 4-39 (Cont.) CNE 23.3.1 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
			to 23.2.0, configure the index management policy for OpenSearch Dashboard before performing an upgrade. For procedure, see the "*Configuring Index Management Policy for OpenSearch Dashboard*" section in 23.2.0 *Oracle Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide*.		

Table 4-39 (Cont.) CNE 23.3.1 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35743643	CNE User Guide - Add terraform plan command for any modification of Worker Nodes	A terraform plan command must be run before running the script for modifying worker node, such as creating or deleting worker nodes. Users have requested to include this terraform plan command in the CNE user documentation.	Whenever the host inventory is called or generated (for example: `./hosts --hostfile`), the inventory is recreated using all the copies of the `terraform.tfstate` present in the cluster directory including the backup. This inventory could have instances from the correct tfstate plus all the instances from the backup file. This could lead to creating duplicates and effectively re-adding any deleted node. **Workaround**: Update the `terraform plan` command for any modification of worker nodes including creation or deletion. This command must be run before running the script mentioned in the procedures.	2	23.1.0

Table 4-39 (Cont.) CNE 23.3.1 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35426047	removeWorkerNode.py not targeting node (Openstack)	While running the automated script to remove a Kubernetes worker node, the script does not target the specific node (given as an argument) while calling terraform. This causes terraform to always delete the last worker node from its list, instead of the targeted node.	Running the procedure for any node other than the last one causes terraform to delete the wrong node. However, the correct node gets deleted from the Kubernetes node list and LB controller configuration. This leaves the cluster in an unhealthy state in which neither of the affected nodes is correctly removed. **Workaround**: Do not use the Removing a Worker Node script to remove a worker node. If the procedure is already run and the cluster is in an unhealthy state, perform the following steps: • Manually remove the correct targeted node using terraform. • Manually remove the other impacted node (last in the list) from the LB Controller and Kubernetes.	3	23.2.0

OSO 23.3.1

There are no known bugs in this release.

4.3.4 cnDBTier Known Bugs

cnDBTier Release 23.3.3

Table 4-40 cnDBTier 23.3.3 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36234344	With BSF DB 23.2.2.0.0 upgrade, ndbmysqld all pods are restarting frequently.	While performing a cnDBTier upgrade, all `ndbmysqld` pods restart frequently.	mysqld georeplication pods restart when it detects that the binlog injector thread is stalled. However, the automatic action results in a replication channel swicthover and georeplication continues. There is no impact to customer traffic due to the restart of mysqld georeplication. **Workaround:** The system performs the workaround automatically. The system restarts the mysqld geo replication pods when the code monitoring code detects that the bin log injector thread is stalled to prevent impact on the customer traffic.	2	23.2.2
36487409	dbtpasswd doesn't retain the old password in some of the pods	The `dbtpasswd` script doesn't retain the old password in some of the pods.	Application pods with old password may not be able to connect to cnDBTier database. The connection depends on the mysqld pod that is used to attempt the connection. If the mysqld pod is one of the affected pods, then the connection fails. **Workaround:** Restart the application pods with the old passwords, so that the pods get the new password from Kubernetes secret.	3	23.4.2

cnDBTier Release 23.3.2

There are no known bugs in this release.

cnDBTier Release 23.3.1

There are no known bugs in this release.

cnDBTier Release 23.3.0

Table 4-41 cnDBTier 23.3.0 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 NEF Known Bugs

NEF 23.3.2 Known Bugs

There are no known bugs in this release.

NEF 23.3.1 Known Bugs

There are no known bugs in this release.

Table 4-42 NEF 23.3.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35753399	Collision of Reference-Number Diameter AVP in Device Trigger create subscription flow	While creating a Device Trigger transaction flow, there is a probability of collision on the Reference-Number Diameter AVP value that leads to 4xx error response. The higher TPS for Device Trigger Create transactions increase the probability of collision.	The device trigger subscriptions are not created intermittently. **Workaround**: Reattempt to create a successful subscription.	3	23.3.0
35722356	Getting intermittent BlackListIpException errors in one NEF microservice while inservice upgrade from 23.2.0 to 23.3.0	While performing an in-service upgrade from NEF 23.2.0 to 23.3.0, an intermittent issue was identified which occurred due to certain conditions.	`BlackListIpException` might be raised for the requests in *fivegc* agent pods that results in service disruption. This is an intermittent issue, which may not occur for all the requests. **Workaround**: Manually remove the *fivegc* agent pod that is printing `BlackListIpException`.	3	23.3.1

Table 4-42 (Cont.) NEF 23.3.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35753770	Getting intermittent BlackListIpException errors in one NEF microservice while inservice rollback from 23.3.0 to 23.1.0	While performing an in-service rollback from NEF 23.3.0 to 23.1.0, an intermittent issue was identified which occurred due to certain conditions.	`BlackListIpException` might be raised for the requests in *fivegc* agent pods that results in service disruption. This is an intermittent issue which may not occur for all the requests. **Workaround**: Manually remove the *fivegc* agent pod that is printing `BlackListIpException`.	3	23.3.0

4.3.6 NRF Known Bugs

NRF 23.3.2 Known Bugs

There are no new known bugs in this release. All the bugs from the previous release are applicable to this release.

NRF 23.3.1 Known Bugs

There are no new known bugs in this release. All the bugs from the previous release are applicable to this release.

Table 4-43 NRF 23.3.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36137134	During NRF rollback from 23.4.0 to 23.3.1, restarts are observed in perf-info pods	During rollback from 23.4.0 to 23.3.1, restart can be observed in perf-info pod. However the PODs will eventually comeup post restart.	No customer impact. The pod will automatically come up post restart. **Workaround**: None	2	23.3.0
35735394	Randomly Config Pod getting restarted on fresh install/upgrade	During fresh installation and upgrade, the NRF configuration pod is restarting in some instances.	Configuration pod gets stable after a few restarts. **Workaround**: No workaround available	3	23.3.0
34205871	3gpp-Sbi-Correlation-Info header not populated in response generated from IGW and NRF microservices framework	3gpp-Sbi-Correlation-Info header is not populated in the response generated from the Ingress Gateway and NRF microservices framework.	It can occur in a rare scenario or overload cases. **Workaround**: It can occur in a rare scenario or overload cases.	4	22.2.0
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 attribute values with a plus sign or space, which generates a null pointer in NRF forwarding use cases.	NRF forwarding fails with attribute values with space or plus sign. **Workaround**: NFDiscover service operation query must not have space or a plus sign in any attribute value.	4	22.2.0

Table 4-43 (Cont.) NRF 23.3.0 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 has servicename query parameter with one servicename, during the load calculation for discoveryResultLoadThreshold, NRF must consider the NFService level load, if present. Else, it will consider NFProfile level load. If servicename query parameter is not present, it will use the default configured load (defaultLoad). NRF is not considering the calculated load for discoveryResultLoadThreshold feature when the load of the NFProfile is null and there is one NFService 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**: No workaround available. This issue occurs only when discoveryResultLoadThreshold feature is enabled.	4	1.15.0

Table 4-43 (Cont.) NRF 23.3.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35763211	App-info does not detect alerts with OSO for infra-validation	When NRF performs infrastructure validation during installation or upgrade, it checks for the presence of critical alerts in the system. With OSO, the detection of alerts fails, and the installation or upgrade is considered as success, even if critical alerts are present.	Installation or upgrade of NRF will continue even if critical alerts are present. **Workaround**: Installation or upgrade of NRF will continue even if critical alerts are present.	4	1.15.0

4.3.7 NSSF Known Bugs

Table 4-44 NSSF 23.3.1 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35368483	NSSF should reject the roaming scenarios because of roaming is not supported	NSSF does not provide support for roaming use cases. Specifically, Information Elements (IEs), which are optional and related to roaming, are ignored by NSSF.	There is no loss of service as the SBI message remains unaffected. Any additional Information Elements (IEs) are simply ignored. **Workaround**: No workaround available	3	23.1.0

Table 4-44 (Cont.) NSSF 23.3.1 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35661263	NSSF is sending subscription response with IE "3gpp-Sbi-Binding" when feature flag is disable "Indirect communication" NSSF 23.2.0	NSSF must not respond with the 3gpp-Sbi-Binding header when the Indirect Communication feature is disabled. Currently, NSSF does not include or process this header when the Helm flag is set to false. However, there are instances where the incorrect header name is included in the response due to lack of validation.	There is no loss of traffic. However, an incorrect header is included in the response. **Workaround**: No workaround available	3	23.2.0
35590771	NSSF 23.2.0 : Align error codes with 29.500	NSSF is responding with an improper error cause code in scenarios involving the NsSelection GET. Since the request is a GET API, and the URL parameters, although presented as JSON, essentially function as query parameters (request parameters), the cause code must include the keyword "QUERY."	This applies only in corner cases, and even in those situations, the response code is correct. The issue lies specifically in the error cause code, with no traffic loss. The result code remains the same. It is the error cause code that needs to be addressed. **Workaround**: No workaround available	3	23.2.0

Table 4-44 (Cont.) NSSF 23.3.1 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35616274	NSSF 23.2: The authorizedNssaiAvailabilityData includes sNSSAIs that are restricted in the TAC	NSSF responds with a 200 status code when AMF sends an update in a scenario where all TAI-SNSSAI combinations are restricted. NSSF should respond with a 403 error code (SNSSAI_NOT_SUPPORTED) when AMF sends an NsAvailability update indicating supported SNSSAIs per TAI, and NSSF is configured in a way that restricts all SNSSAI-TAI combinations.	The scenario is a corner case because it's rare for an NSSF to be configured in a way that restricts all SNSSAI-TAI combinations. Typically, NSSF configurations allow at least some SNSSAI-TAI combinations, even if it's a small number. AMF sends an NsAvailability update to the NSSF, indicating its support for a specific set of SNSSAIs per TAI. However, the NSSF cannot support any of these SNSSAIs because all SNSSAI-TAI combinations are restricted in its configuration. This situation leads to the issue of incorrect responses and may cause operational challenges. **Workaround**: No workaround available	3	23.2.0

Table 4-44 (Cont.) NSSF 23.3.1 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35701446	Getting 500 internal error in nsavailibility pod when operator tries to change nssai value after patch add operation	In a specific scenario, there is an intermittent issue where the NSSF subscription service fails to send notification updates. This situation occurs when two Tai Ranges are configured in a subscription, followed by a patch to add a subscription for a single TAC. This occurs when the TAC range is up to 999999. If the TAC range exceeds 999999, a configuration update fails to trigger a notification.	The impact of this issue is minimal. **Workaround**: No workaround available	3	23.2.0
35699787	Error statement for existing subscriber for tac 9999 & 999999 is different	NSSF supports subscriptions, where each subscription comprises a Tai list. According to the specifications, Tai should not be duplicated. If a subscription is created with a duplicate Tai, NSSF rejects the message with a 400 Bad Request status.	There is no loss of service as the error code is accurate. **Workaround**: No workaround available	3	23.2.0

Table 4-44 (Cont.) NSSF 23.3.1 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35701232	"422 Bad Request Error Jason" even on not giving proper path value in PATCH request	NSSF supports subscriptions and allows patches to be applied to them. However, in a specific scenario, when a subscription is established and a patch is attempted on the subscription with an incomplete path, NSSF rejects the patch with a 422 response.	There is no loss of service as the error code is accurate. **Workaround**: No workaround available	3	23.2.0
35684393	NSSF 23.2 allowedNssaiList not in response when configuredsnssai has defaultIndication=true	This issue arises in a specific scenario where NSSF sends only ConfiguredNSSAI without sending AllowedNSSAI. This occurs when none of the SNSSAIs, which form the intersection of RequestedNSSAI and SubscribedNSSAI, are allowed in the TAI where the UE is located. Additionally, there is a default configured SNSSAI that is absent from the RequestedNSSAI but is allowed for the TAI in which the UE is situated.	There is minimal loss of service as this scenario is rare. **Workaround**: No workaround available	3	23.2.0

Table 4-44 (Cont.) NSSF 23.3.1 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35553567	Reroute count not working as expected for routesconfiguration((Support for SCP Health API using HTTP2 OPTIONS))	The number of times the Egress Gateway attempts to reroute after encountering an error is configured using routesconfiguration parameter. However, when this parameter is set to 1, the notification attempts routing twice.	There is a minor impact on traffic as rerouting occurs only in response to errors. **Workaround**: No workaround available	3	23.2.0
35624980	Site-1 does not remove the NS-Availability data from the nssfProvSite-1DB.tai_range_snssai_list_map table if NSSAI and taiRangeList have configured by the operator.	The replication process deletes the content in both site-1 and site-2 resulting in stale entries in the helper tables.	The helper tables store temporary data during the replication process. They do not hold any live traffic data, hence they do not directly affect traffic. Once the configuration between the two sites is synchronized and the replication process restarts, the helper tables become unnecessary and can be removed. The configuration will be restored from the live traffic data present in the production databases. **Workaround**: No workaround available	3	23.2.0

Table 4-44 (Cont.) NSSF 23.3.1 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35624271	2-site GR setup ASM Enabled: Site-2 does not delete the NS-Availability information on the nssfProvSite-2DB.nss rule and nssai auth tables, while Site-1 deletes the NS-Availability	The replication process deletes the content in both site-1 and site-2 resulting in stale entries in the helper tables.	The helper tables store temporary data during the replication process. They do not hold any live traffic data, hence they do not directly affect traffic. Once the configuration between the two sites is synchronized and the replication process restarts, the helper tables become unnecessary and can be removed. The configuration will be restored from the live traffic data present in the production databases. **Workaround**: No workaround available	3	23.2.0

Table 4-44 (Cont.) NSSF 23.3.1 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35638572	Discrepancy in statistics with NSSF 23.2.0 (Indirect communication)	The following metrics are not present in Prometheus: • ocnssf_nssaiavailability_indirect_communication_rx • ocnssf_nssaiavailability_indirect_communication_tx • ocnssf_nssaiavailability_notification_indirect_communication_tx • ocnssf_nssaiavailability_indirect_communication_subscription_failure • ocnssf_nssaiavailability_indirect_communication_notification_failure Also, ocnssf_nssaiavailability_notification_indirect_communication_rx_total in Prometheus does not match with the metric	There is no traffic impact and no loss of service. **Workaround**: No workaround available	3	23.2.0

Table 4-44 (Cont.) NSSF 23.3.1 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
		name documented in the user guide, `ocnssf_nssaiavailability_notification_indirect_communication_rx`.			
35502848	Out of Range Values are being configured in PeerMonitoringConfiguration (Support for SCP Health API using HTTP2 OPTIONS)	The parameters such as timeout, frequency, failureThreshold, and successThreshold in PeerMonitoringConfiguration should be set within the specified maximum and minimum limits.	There is no traffic impact and no loss of service. **Workaround**: No workaround available	3	23.2.0

Table 4-44 (Cont.) NSSF 23.3.1 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35705005	NSSF not sending Failure for 2nd received ns-availability PUT response if Tai Range overlap is there	NSSF allows scenarios where two AMFs simultaneously support overlapping TAI range configurations. This occurs when a particular section of the configuration is already limited by the operator. NSSF should reject second AMF's request due to the overlapping range, but it accepts the request.	This is a rare scenario where the operator configures a single TAC range shared by two distinct AMF sets. Additionally, two AMFs from different sets support the same SNSSAIs within these TAC ranges. These AMFs send NsAvailability PUT requests with identical SNSSAIs and mappings of TAI ranges. Consequently, there is a potential for incorrect configuration as NSSF accepts this configuration despite the overlap. **Workaround**: Configure NSSF with TAI ranges that are restricted within a PLMN. This ensures when two AMFs originating from different sets transmit an Availability PUT with intersecting TAI ranges.	3	23.2.0
35297857	If AMF and NSSF enabled ONSSAI feature, NSSF should reject the ns-availability subscriptions request when taiList IE is non-empty array in ns-availability subscriptions request.	NSSF supports both Tai list and TaiRange list. However, there is a discrepancy in the specifications if both should be supported or not.	There is no traffic impact and no loss of service. **Workaround**: No workaround available.	4	23.1.0

Table 4-44 (Cont.) NSSF 23.3.1 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35394240	CandidateAmfList is not added by NSSF when No AMF is sending the ns-availability update request to NSSF	CandidateAmfList is not added by NSSF when No AMF is sending the ns-availability update request to NSSF	The PLMN Level Profile (Default profile) is associated with an operator-configured rule. However, AMFs are not transmitting availability updates, resulting in the absence of any mapping of an AMF set to that particular profile. This scenario results in a situation where no AMF set is linked or connected. **Workaround**: The operator should configure a rule and establish a mapping using a Network Slice profile instead of a default PLMN profile.		
35709940	NSSF 23.1.0 GrSite feature not exposing DELETE Method to remove a GR site	NSSF supports the use of the PUT method on managed object (GrSite), enabling the customers to remove a site from the NSSF GR site setup. There is also a requirement to support the DELETE method on the same managed object.	There is no traffic impact as the task of removing a site involves setting it to "down". Additionally, since PUT is supported, the siteId can also be updated. **Workaround**: No workaround available	4	23.1.0

Table 4-45 NSSF 23.3.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35368483	NSSF should reject the roaming scenarios because of roaming is not supported	NSSF does not provide support for roaming use cases. Specifically, Information Elements (IEs), which are optional and related to roaming, are ignored by NSSF.	There is no loss of service as the SBI message remains unaffected. Any additional Information Elements (IEs) are simply ignored. **Workaround**: No workaround available	3	23.1.0
35661263	NSSF is sending subscription response with IE "3gpp-Sbi-Binding" when feature flag is disable "Indirect communication" NSSF 23.2.0	NSSF must not respond with the 3gpp-Sbi-Binding header when the Indirect Communication feature is disabled. Currently, NSSF does not include or process this header when the Helm flag is set to false. However, there are instances where the incorrect header name is included in the response due to lack of validation.	There is no loss of traffic. However, an incorrect header is included in the response. **Workaround**: No workaround available	3	23.2.0

Table 4-45 (Cont.) NSSF 23.3.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35701446	Getting 500 internal error in nsavailibility pod when operator tries to change nssai value after patch add operation	In a specific scenario, there is an intermittent issue where the NSSF subscription service fails to send notification updates. This situation occurs when two Tai Ranges are configured in a subscription, followed by a patch to add a subscription for a single TAC. This occurs when the TAC range is up to 999999. If the TAC range exceeds 999999, a configuration update fails to trigger a notification.	The impact of this issue is minimal. **Workaround**: No workaround available	3	23.2.0
35699787	Error statement for existing subscriber for tac 9999 & 999999 is different	NSSF supports subscriptions, where each subscription comprises a Tai list. According to the specifications, Tai should not be duplicated. If a subscription is created with a duplicate Tai, NSSF rejects the message with a 400 Bad Request status.	There is no loss of service as the error code is accurate. **Workaround**: No workaround available	3	23.2.0

Table 4-45 (Cont.) NSSF 23.3.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35701232	"422 Bad Request Error Jason" even on not giving proper path value in PATCH request	NSSF supports subscriptions and allows patches to be applied to them. However, in a specific scenario, when a subscription is established and a patch is attempted on the subscription with an incomplete path, NSSF rejects the patch with a 422 response.	There is no loss of service as the error code is accurate. **Workaround**: No workaround available	3	23.2.0
35684393	NSSF 23.2 allowedNssaiList not in response when configuredsnssai has defaultIndication=true	This issue arises in a specific scenario where NSSF sends only ConfiguredNSSAI without sending AllowedNSSAI. This occurs when none of the SNSSAIs, which form the intersection of RequestedNSSAI and SubscribedNSSAI, are allowed in the TAI where the UE is located. Additionally, there is a default configured SNSSAI that is absent from the RequestedNSSAI but is allowed for the TAI in which the UE is situated.	There is minimal loss of service as this scenario is rare. **Workaround**: No workaround available	3	23.2.0

Table 4-45 (Cont.) NSSF 23.3.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35553567	Reroute count not working as expected for routesconfiguration((Support for SCP Health API using HTTP2 OPTIONS))	The number of times the Egress Gateway attempts to reroute after encountering an error is configured using routesconfiguration parameter. However, when this parameter is set to 1, the notification attempts routing twice.	There is a minor impact on traffic as rerouting occurs only in response to errors. **Workaround**: No workaround available	3	23.2.0
35624980	Site-1 does not remove the NS-Availability data from the nssfProvSite-1DB.tai_range_snssai_list_map table if NSSAI and taiRangeList have configured by the operator.	The replication process deletes the content in both site-1 and site-2 resulting in stale entries in the helper tables.	The helper tables store temporary data during the replication process. They do not hold any live traffic data, hence they do not directly affect traffic. Once the configuration between the two sites is synchronized and the replication process restarts, the helper tables become unnecessary and can be removed. The configuration will be restored from the live traffic data present in the production databases. **Workaround**: No workaround available	3	23.2.0

Table 4-45 (Cont.) NSSF 23.3.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35638572	Discrepancy in statistics with NSSF 23.2.0 (Indirect communication)	The following metrics are not present in Prometheus: • `ocnssf_nssaiavailability_indirect_communication_rx` • `ocnssf_nssaiavailability_indirect_communication_tx` • `ocnssf_nssaiavailability_notification_indirect_communication_tx` • `ocnssf_nssaiavailability_indirect_communication_subscription_failure` • `ocnssf_nssaiavailability_indirect_communication_notification_failure` Also, `ocnssf_nssaiavailability_notification_indirect_communication_rx_total` in Prometheus does not match with the metric	There is no traffic impact and no loss of service. **Workaround**: No workaround available	3	23.2.0

Table 4-45 (Cont.) NSSF 23.3.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
		name documented in the user guide, `ocnssf_nssaiavailability_notification_indirect_communication_rx`.			
35502848	Out of Range Values are being configured in PeerMonitoringConfiguration (Support for SCP Health API using HTTP2 OPTIONS)	The parameters such as timeout, frequency, failureThreshold, and successThreshold in PeerMonitoringConfiguration should be set within the specified maximum and minimum limits.	There is no traffic impact and no loss of service. **Workaround**: No workaround available	3	23.2.0

Table 4-45 (Cont.) NSSF 23.3.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35705005	NSSF not sending Failure for 2nd received ns-availability PUT response if Tai Range overlap is there	NSSF allows scenarios where two AMFs simultaneously support overlapping TAI range configurations. This occurs when a particular section of the configuration is already limited by the operator. NSSF should reject second AMF's request due to the overlapping range, but it accepts the request.	This is a rare scenario where the operator configures a single TAC range shared by two distinct AMF sets. Additionally, two AMFs from different sets support the same SNSSAIs within these TAC ranges. These AMFs send NsAvailability PUT requests with identical SNSSAIs and mappings of TAI ranges. Consequently, there is a potential for incorrect configuration as NSSF accepts this configuration despite the overlap. **Workaround**: Configure NSSF with TAI ranges that are restricted within a PLMN. This ensures when two AMFs originating from different sets transmit an Availability PUT with intersecting TAI ranges.	3	23.2.0

Table 4-45 (Cont.) NSSF 23.3.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35368483	NSSF should reject the roaming scenarios because of roaming is not supported	NSSF does not support roaming use cases and disregards the optional Information Elements (IEs) related to roaming.	There is no loss of service as the SBI message is unaffected. Any additional Information Elements (IEs) is simply disregarded. **Workaround**: No workaround available	3	23.1.0
35624271	2-site GR setup ASM Enabled: Site-2 does not delete the NS-Availability information on the nssfProvSite-2DB.nssrule and nssai auth tables, while Site-1 deletes the NS-Availability	The replication process deletes the content in both site-1 and site-2 resulting in stale entries in the helper tables.	The helper tables store temporary data during the replication process. They do not hold any live traffic data, hence they do not directly affect traffic. Once the configuration between the two sites is synchronized and the replication process restarts, the helper tables become unnecessary and can be removed. The configuration will be restored from the live traffic data present in the production databases. **Workaround**: No workaround available	3	23.2.0

Table 4-45 (Cont.) NSSF 23.3.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35709940	NSSF 23.1.0 GrSite feature not exposing DELETE Method to remove a GR site	NSSF supports the use of the PUT method on managed object (GrSite), enabling the customers to remove a site from the NSSF GR site setup. There is also a requirement to support the DELETE method on the same managed object.	There is no traffic impact as the task of removing a site involves setting it to "down". Additionally, since PUT is supported, the siteId can also be updated. **Workaround**: No workaround available	4	23.1.0
35297857	If AMF and NSSF enabled ONSSAI feature, NSSF should reject the ns-availability subscriptions request when taiList IE is non-empty array in ns-availability subscriptions request.	NSSF supports both Tai list and TaiRange list. However, there is a discrepancy in the specifications if both should be supported or not.	There is no traffic impact and no loss of service. **Workaround**: No workaround available	423.1.0	

Table 4-45 (Cont.) NSSF 23.3.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35394240	CandidateAmfList is not added by NSSF when No AMF is sending the ns-availability update request to NSSF	CandidateAmfList is not added by NSSF when No AMF is sending the ns-availability update request to NSSF	The PLMN Level Profile (Default profile) is associated with an operator-configured rule. However, AMFs are not transmitting availability updates, resulting in the absence of any mapping of an AMF set to that particular profile. This scenario results in a situation where no AMF set is linked or connected. **Workaround**: The operator should configure a rule and establish a mapping using a Network Slice profile instead of a default PLMN profile.		

4.3.8 SCP Known Bugs

SCP 23.3.2 Known Bugs

There are no new known bugs in this release. For existing known bugs, see Table 4-46.

SCP 23.3.1 Known Bugs

There are no new known bugs in this release. For existing known bugs, see Table 4-46.

Table 4-46 SCP 23.3.0 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

4.3.9 SEPP Known Bugs

Table 4-47 SEPP 23.3.2 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
36026779	EGW restart observed	Gateway restart is observed at the capacity of 5000 MPS per pod. As an interim and temporary measure, the supported MPS per pod is reduced to 3200, the resource profile and dimensioning sheet is updated to reflect this updated value.	Overall system throughput has been reduced to 54 K MPS with an increased pod count. The per pod throughput has been reduced to 3200 MPS from 5000 MPS.Workaround: None	3	23.3.0

Table 4-47 (Cont.) SEPP 23.3.2 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
36035492	PLMN IGW restarts due to java.lang.OutOfMemoryError	Gateway restarts are observed at advertised capacity of 5000 MPS/POD and plmn ingress gateway starts throwing out of memory issue resulting in restarting the service. As an interim and temporary measure, the supported MPS per pod is reduced to 3200, the resource profile and dimensioning sheet is updated to reflect this updated value.	Overall System throughput has been reduced to 54 K MPS with an increased pod count. The per pod throughput has been reduced to 3200 MPS from 5000.Workaround: None	3	23.3.1
35527387	DNS SRV Support- Loss of SEPP forwarding Traffic at IGW with DNS SRV enabled at high TPS	Gateway restarts are observed at the capacity of 5000 MPS/POD and plmn ingress gateway starts throwing out of memory issue resulting in restarting the service. As an interim and temporary measure, the supported MPS per pod is reduced to 3200, the resource profile and dimensioning sheet is updated to reflect this updated value.	Overall System throughput has been reduced to 54 K MPS with an increased pod count. The per pod throughput has been reduced to 3200 MPS from 5000.Workaround: None	3	23.2.3

SEPP 23.3.1 Known Bugs

There are no known bugs in this release.

Table 4-48 SEPP 23.3.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
35745233	Log messages from pods are intermittently not reaching the openSearch	On fresh installation, all the logs from all the SEPP services are available in OpenSearch. But, after some time, logs from none of the services are observed in OpenSearch, whereas logs are present in the pod.	Logs are not visible in OpenSearch Dashboard. **Workaround**: For workaround: 1. See the Resource Requirements for fluent bit in Cloud Native Environment (CNE) Installation, Upgrade, and Fault Recovery Guide. 2. Restart the fluent bit pods.	2	23.2.0

Table 4-48 (Cont.) SEPP 23.3.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
35036599	[SEPP-APIGW] Total traffic loss after upgrade when global Ingress rate limiting feature is enabled	There is a total traffic failure when there is an upgrade from the previous SEPP release to 23.3.x and Rate Limit feature is enabled. The following exception is noticed after the upgrade. `Role=SpringframeworkBootLoaderJarLauncher)) io.github.bucket4j.BucketConfiguration; class invalid for deserialization","message":"(Wrapped: Failed request execution for MapDistCache service on Member(Id=2)` However, the traffic remains unaffected if the ingress pod is restarted.	If Global Rate Limiting feature is enabled and there is a traffic while upgrading to any release, after the upgrade, the n32-ingress-gateway stops processing the traffic. There will be total traffic loss. **Workaround**: Following are the three workaround scenarios: 1. If SBI traffic is in progress during the upgrade, after the upgrade, restart the n32-ingress-gateway. The system will recover and start processing the traffic. 2. Perform an upgrade with Global Rate	2	22.4.0

Table 4-48 (Cont.) SEPP 23.3.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
			Limiting feature disabled. 3. Perform an upgrade to 23.1.0 without traffic.		

Table 4-48 (Cont.) SEPP 23.3.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
35764279	Upgrade/ Rollback for Performance pod failing with CDCS	While performing an upgrade from SEPP source release to 23.3.0 (with Perf-info version 23.3.1), the performance pod is behaving abnormally. • In some cases, it does not come up and after 11 retries, it goes into crashloopback state. • In some cases, it becomes active after 3-4 retries. This is due to the --wait parameter added by CDCS when Helm upgrade or rollback is run through CDCS pipeline. This parameter ensures that the steps are run in serial manner, which in turn raises a deadlock condition. This issue does not allow post upgrade or post rollback steps to be run, resulting in instability of setup.	Upgrade and rollback with CDCS fail. **Workaround**: For workaround: 1. Run Helm upgrade or rollback through command line. 2. Once pre rollback steps are completed and pod restarts for perf-info, manually edit the deployment and update the following PROBE_VALIDATION_BYPASS flag to true by using kubectl edit deploy command: - name:	2	23.3.0

Table 4-48 (Cont.) SEPP 23.3.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
			`PROBE_VALIDATION_BYPASS value: "true"`		
35744748	Coherence service restarting once/twice during installation	During the installation, coherence service is getting restarted, but is up and running after one or two attempts.	No impact **Workaround**: In case service goes in crashloopback state, delete the coherence-svc pod using this command: `kubectl delete po -n <namespace> <release name-coherence-svc-pod>`	3	23.3.0

Table 4-48 (Cont.) SEPP 23.3.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
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	This scenario is observed when Egress Gateway is not able to send the SBI message to next node or NF when the NF is unreachable. The HTTP error reason in the response received by gateway is not correct. error-reason: `org.springframework.web.reactive.function.client.WebClientRequestException: nested exception is java.nio.channels.ClosedChannelException`	The user will not able to identify the reason of failure from the error reason. They have to check the Grafana and metrics to find the root cause. **Workaround** : Run kubectl command to verify that all the services are up and running. Wait for the services to be up and running and the issue will get resolved.	3	22.2.0
35767064	Rollback failed from 23.3.0 to lower versions with error : no ConfigMap with the name "rss-ratelimit-map" found.	SEPP rollback failed from 23.3.0 to lower releases (23.1.x and 23.2.x) with Error: no ConfigMap with the name "rss-ratelimit-map" found. This is a Helm issue where configMap is already present, but Helm considers it as not present and results in an error.	SEPP rollback will fail. **Workaround** : Run the Helm rollback command again with `--force` option and rollback will run without any issue.	3	23.2.0

Table 4-48 (Cont.) SEPP 23.3.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
35767215	SEPP upgrade fails when executed for second time after performing rollback	When the upgrade is performed to SEPP release 23.3.0 more than once after performing a rollback, the upgrade fails with the following error: `Error: UPGRADE FAILED: rendered manifests contain a resource that already exists. Unable to continue with update: ConfigMap "egress-ratelimit-map" in namespace "yash-upgrade" exists and cannot be imported into the current release: invalid ownership metadata; label validation error: missing key "app.kubernetes.io/managed-by": must be set to "Helm"; annotation validation error: missing key "meta.helm.sh/release-name": must be set to "ocsepp-release"; annotation`	SEPP upgrade will fail. **Workaround** : Delete the 'egress-ratelimit-map' config map before upgrading SEPP for second time. `kubectl delete cm -n <namespace> egress-ratelimit-map`	3	23.3.0

Table 4-48 (Cont.) SEPP 23.3.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
		`validation error: missing key "meta.helm.sh/release-namespace": must be set to "yash-upgrade"` Upgrade/Rollback Path: 23.1.3 upgraded to 23.3.0 and rollback to 23.1.3 and upgrade to 23.3.0 and upgrade fails at this point.			
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 Remote SEPP, error code 204 is returned but the entry is not deleted. No error is displayed when POST request is run while the pods are scaled down.	No impact. Run the Delete command when all the pods and services are up and running. **Workaround**: Wait for the pods and services to be up and running. Run the delete command, and it will be successful.	4	22.3.0

4.3.10 UDR Known Bugs

UDR 23.3.2 Known Bugs

There are no known bugs in this release.

Table 4-49 UDR 23.3.1 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
34745401	User Agent Header is present in UDR EGW messages even when configuration flag is set to false	User-Agent header is added by default in the Egress Gateway messages even when the configuration flag is set to false.	No impact **Workaround**: No workaround available	3	22.3.1
35547132	SLF - In NF scoring feature App Info is not periodically fetching the NF score as per default timer	Network Function (NF) score calculation logs are not refreshed periodically as per the default time.	No impact **Workaround**: NF score should be refreshed at 30 seconds.	3	23.2.0
35546979	SLF - In NF scoring feature, Scoring type parameter in Custom criteria are accepting values other than ratio and weightage	In the NF Scoring feature, the scoring type is accepting values other than ratio and weightage.	It only has an impact when the customer defines a custom criteria for NF Scoring feature. There is no impact for default NF scoring parameters. **Workaround**: No workaround available	3	23.2.0
35762491	Diameter Gateway metric validation for missing avp in SNA and PUA response is getting pegged twice	Metric validation on Diameter Gateway is pegged twice for the missing Attribute Value Pair (AVP).	There is no impact. Metrics need to be ignored for this test case. **Workaround**: No workaround available	3	23.3.0

Table 4-49 (Cont.) UDR 23.3.1 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35762463	VSA PUT not merging the subscriber keys when ondemand enabled	When on-demand migration is enabled, VSA PUT operation does not merge with the subscriber keys.	No impact **Workaround**: Subscriber keys must be manually added by additional PUT operation from the provisioning system.	3	23.3.0

Table 4-50 UDR 23.3.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
34745401	User Agent Header is present in UDR EGW messages even when configuration flag is set to false	User-Agent header is added by default in the Egress Gateway messages even when the configuration flag is set to false.	No impact **Workaround**: No workaround available	3	22.3.1
35547132	SLF - In NF scoring feature App Info is not periodically fetching the NF score as per default timer	Network Function (NF) score calculation logs are not refreshed periodically as per the default time.	No impact **Workaround**: NF score should be refreshed at 30 seconds.	3	23.2.0

Table 4-50 (Cont.) UDR 23.3.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35546979	SLF - In NF scoring feature, Scoring type parameter in Custom criteria are accepting values other than ratio and weightage	In the NF Scoring feature, the scoring type is accepting values other than ratio and weightage.	It only has an impact when the customer defines a custom criteria for NF Scoring feature. There is no impact for default NF scoring parameters. **Workaround**: No workaround available	3	23.2.0
35762439	Retrieving quota with name and cid failing on VSA APIs where subscriber has mk1 and 4g quota	When subscriber has mk1 and 4G quota, retrieving quota with name and CID fails on Vendor Specific Attribute (VSA) APIs.	When subscriber has mk1 and 4G quota, retrieving quota with name and CID fails on Vendor Specific Attribute (VSA) APIs. **Workaround**: No workaround available	3	23.3.0
35762463	VSA PUT not merging the subscriber keys when ondemand enabled	When on-demand migration is enabled, VSA PUT operation does not merge with the subscriber keys.	No impact **Workaround**: Subscriber keys must be manually added by additional PUT operation from the provisioning system.	3	23.3.0

Table 4-50 (Cont.) UDR 23.3.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35762491	Diameter Gateway metric validation for missing avp in SNA and PUA response is getting pegged twice	Metric validation on Diameter Gateway is pegged twice for the missing Attribute Value Pair (AVP).	There is no impact. Metrics need to be ignored for this test case. **Workaround**: No workaround available	3	23.3.0
35762518	ProvGW Egress Gateway is not propagating the Trace ID to UDR Ingress Gateway	Provisioning Gateway's Egress Gateway is not propagating the Trace ID to UDR's Ingress Gateway.	There is no impact. Trace ID from the previous hop is lost. **Workaround**: No workaround available	3	23.3.0

4.3.11 Common Services Known Bugs

4.3.11.1 Egress Gateway Known Bugs

Release 23.3.x

Table 4-51 Egress Gateway 23.3.x Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35750717	OpenTelemetry : ProvGW Egress Gateway is not propagating the Trace ID to UDR Ingress Gateway	Jaeger tracing does not show span propagation in the DEBUG mode when the traffic flow is from provEGW to UDR Ingress Gateway.	No impact **Workaround**: No workaround is available. The issue will be resolved in the next gateway release.	3	23.3.3

Table 4-51 (Cont.) Egress Gateway 23.3.x Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35527387	[SEPP-APIGW] DNS SRV Support-Loss of SEPP forwarding Traffic at IGW with DNS SRV enabled at high TPS	When DNS SRV service is enabled with ARS, high latency is observed when testing traffic load beyond 2.1K TPS per pod.	Traffic will timeout if the sustained load beyond 2.1K TPS is injected to Engress Gateway when the DNS SRV feature is enabled. **Workaround**: Limit the load per Egress Gateway to not exceed 2K TPS per pod when the DNS SRV feature is enabled. Add more Egress Gateway pods if more traffic is to be processed.	2	23.2.3

4.3.11.2 Ingress Gateway Known Bugs

Ingress Gateway 23.3.x Known Bugs

There are no known bugs in this release.

4.3.11.3 NRF-Client Known Bugs

Release 23.3.0

There are no known bugs in this release.

4.3.11.4 ATS Known Bugs

Release 23.3.0

There are no known bugs in this release.