Oracle® Communications

Cloud Native Core Release Notes

Release 2.23.2
F82196-39
September 2024

Oracle Communications Cloud Native Core Release Notes, Release 2.23.2

F82196-39

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 2.23.2 - F82196-39, September 2024

CNE 23.2.6 Release

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

Release 2.23.2 - F82196-38, June 2024

UDR 23.2.2 Release

Updated the following sections with the details of UDR release 23.2.2:

- Unified Data Repository (UDR)
- Media Pack
- Compatibility Matrix
- Common Microservices Load Lineup

Release 2.23.2 - F82196-37, March 2024

cnDBTier 23.2.5 Release

Updated the following sections with the details of cnDBTier release 23.2.5:

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

Release 2.23.2 - F82196-36, March 2024

Policy 23.2.8 Release

Updated the following sections with the details of Policy release 23.2.8:

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

Release 2.23.2 - F82196-35, January 2024

UDR 23.2.1 Release

Updated the following sections with the details of UDR release 23.2.1:

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

- UDR Resolved Bugs

Release 2.23.2 - F82196-34, January 2024

NRF 23.2.3 Release

Updated the following sections with the details of NRF release 23.2.3:

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

CNE 23.2.6 Release

Updated the following sections with the details of CNE release 23.2.6:

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

Release 2.23.2 - F82196-33, January 2024

cnDBTier 23.2.4 Release

Updated the following sections with the details of cnDBTier release 23.2.4:

- Cloud Native Core cnDBTier
- Media Pack
- Compatibility Matrix
- Common Microservices Load Lineup
- cnDBTier Resolved Bugs

Release 2.23.2 - F82196-32, January 2024

Policy 23.2.7 Release

Updated the following sections with the details of Policy release 23.2.7:

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

BSF 23.2.4 Release

Updated the following sections with the details of BSF release 23.2.4:

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

Release 2.23.2 - F82196-31, December 2023

SCP 23.2.2 Release

Added a new bug 36070406 in the SCP Resolved Bugs section.

Release 2.23.2 - F82196-30, December 2023

cnDBTier 23.2.3 Release

Updated the following sections with the details of cnDBTier release 23.2.3:

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

Release 2.23.2 - F82196-29, November 2023

Policy 23.2.6 Release

Updated the following sections with the details of Policy release 23.2.6:

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

Release 2.23.2 - F82196-28, November 2023

BSF 23.2.3 Release

Updated the following sections with the details of BSF release 23.2.3:

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

Release 2.23.2 - F82196-27, November 2023

Policy 23.2.5 Release

Updated the following sections with the details of Policy release 23.2.5:

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

Release 2.23.2 - F82196-26, November 2023

CDCS 23.2.2 Release

Updated the following sections with the details of CDCS release 23.2.2:

- Feature Descriptions
- Media Pack
- Compatibility Matrix
- CDCS Known Bugs

CNE 23.2.5 Release

Updated the following sections with the details of CNE release 23.2.5:

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

CNE 23.2.4 Release

Updated the following sections with the details of CNE release 23.2.4:

- Cloud Native Environment (CNE)
- Media Pack

cnDBTier 23.2.0 Release

Updated the Cloud Native Core cnDBTier section with the details of cnDBTier release 23.2.0.

Release 2.23.2 - F82196-25, November 2023

Policy 23.2.5 Release

Updated the following sections with the details of Policy release 23.2.5:

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

Release 2.23.2 - F82196-24, October 2023

SCP 23.2.3 Release

Updated the following sections with the details of SCP release 23.2.3:

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

CNE 23.2.4 Release

Updated the following sections with the details of CNE release 23.2.4:

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

cnDBTier 23.2.0 and 23.2.1 Releases
Updated the following section with the details of cnDBtier release 23.2.0 and 23.2.1:

Added a bug in the cnDBTier Known Bugs section.

Policy 23.2.4 Release
Updated the Policy Resolved Bugs section with bug 35797403.

NEF 23.2.1 Release
Updated the following sections with the details of NEF release 23.2.1:

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

Release 2.23.2 - F82196-23, October 2023

cnDBTier 23.2.2 Release

Updated the following sections with the details of cnDBTier release 23.2.2:

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

NRF 23.2.2 Release

Updated the following sections with the details of NRF release 23.2.2:

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

SEPP 23.2.2 Release

Updated the following sections with the details of SEPP release 23.2.2:

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

Release 2.23.2 - F82196-22, October 2023

CNC Console 23.2.2 Release

Updated the following sections with the details of CNC Console release 23.2.2:

- 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

Policy 23.2.4 Release

Updated the Compatibility Matrix section.

Release 2.23.2 - F82196-21, October 2023

Policy 23.2.4 Release

Updated the following sections with the details of Policy release 23.2.4:

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

Release 2.23.2 - F82196-20, October 2023

BSF 23.2.2 Release

Updated the following sections with the details of BSF release 23.2.2:

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

cnDBTier 23.2.0 and 23.2.1 Releases

Added a bug in the cnDBTier Known Bugs section.

Release 2.23.2 - F82196-19, September 2023

NRF 23.2.1 Release

Updated the following sections with the details of NRF release 23.2.1:

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

CNC Console 23.2.1 Release

Updated the following sections with the details of CNC Console release 23.2.1:

- 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

CNE 23.2.3 Release

Updated the following sections with the details of CNE release 23.2.3:

- Media Pack
- Compatibility Matrix
- CNE Resolved Bugs

Release 2.23.2 - F82196-18, September 2023

Policy 23.2.2 Release

Updated the following section with the details of Policy release 23.2.2:

- Policy Resolved Bugs

Release 2.23.2 - F82196-17, September 2023

SCP 23.2.2 Release

Updated the following sections with the details of SCP release 23.2.2:

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

Release 2.23.2 - F82196-16, August 2023

Policy 23.2.2 Release

Updated the following sections with the details of Policy release 23.2.2:

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

Release 2.23.2 - F82196-15, August 2023

SEPP 23.2.1 Release

Updated the following sections with the details of SEPP release 23.2.1:

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

Release 2.23.2 - F82196-14, August 2023

CDCS 23.2.1 Release

Updated the following sections with the details of CDCS release 23.2.1:

- Feature Descriptions
- Media Pack
- Compatibility Matrix
- Resolved Bug List

Release 2.23.2 - F82196-13, August 2023

Policy 23.2.1 Release

Updated the following sections with the details of Policy release 23.2.1:

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

BSF 23.2.1 Release

Updated the following sections with the details of BSF release 23.2.1:

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

Release 2.23.2 - F82196-12, August 2023

cnDBTier 23.2.1 Release

Updated the cnDBTier Known Bugs section.

cnDBTier 23.2.0 Release

- Corrected the bug number as "35274059" in the cnDBTier Resolved Bugs section.
- Added a bug in the cnDBTier Known Bugs section.

Release 2.23.2 - F82196-11, August 2023

CNE 23.2.1 Release

Updated the following sections with the details of CNE release 23.2.1:

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

SCP 23.2.1 Release

Updated the following sections with the details of SCP release 23.2.1:

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

- SCP Resolved Bugs
- SCP Known Bugs

Release 2.23.2 - F82196-10, July 2023

cnDBTier 23.2.1 Release

Added a new bug in the cnDBTier Resolved Bugs section.

Release 2.23.2 - F82196-09, July 2023

cnDBTier 23.2.1 Release

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

Release 2.23.2 - F82196-08, June 2023

SCP 23.2.0 Release

Added a new bug 35495203 in the SCP Resolved Bugs section.

Release 2.23.2 - F82196-07, June 2023

23.2.0 Release

Added NFs' compatibility with Oracle Communications Network Analytics Data Director (OCNADD) in Compatibility Matrix.

Release 2.23.2 - F82196-06, June 2023

BSF 23.2.0 Release

Updated the following sections with the details of BSF release 23.2.0:

- Binding Support Function (BSF)
- Media Pack
- Compatibility Matrix
- Common Microservices Load Lineup
- Security Certification Declaration
- BSF Resolved Bugs
- BSF Known Bugs

Policy 23.2.0 Release

Updated the following sections with the details of Policy release 23.2.0:

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

- Policy Resolved Bugs
- Policy Known Bugs

Release 2.23.2 - F82196-05, June 2023

UDR 23.2.0 Release

Updated the following section with the details of UDR release 23.2.0:

- UDR Resolved Bugs

Release 2.23.2 - F82196-04, June 2023

CDCS 23.2.0 Release

Updated the following sections with the details of CDCS release 23.2.0:

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

Release 2.23.2 - F82196-03, June 2023

CNE 23.2.0 Release

Updated the following sections with the details of CNE release 23.2.0:

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

Release 2.23.2 - F82196-02, May 2023

ATS 23.2.0 Release

Updated the following section with the details of ATS release 23.2.0:

- Automated Testing Suite (ATS) Framework

SCP 23.2.0 Release

Updated the following sections with the details of SCP release 23.2.0:

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

SEPP 23.2.0 Release

Updated the following sections with the details of SEPP release 23.2.0:

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

UDR 23.2.0 Release

Updated the following sections with the details of UDR release 23.2.0:

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

Release 2.23.2 - F82196-01, May 2023

CNC Console 23.2.0 Release

Updated the following sections with the details of CNC Console release 23.2.0:

- 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

cnDBTier 23.2.0 Release

Updated the following sections with the details of cnDBTier release 23.2.0:

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

NEF 23.2.0 Release

Updated the following sections with the details of NEF release 23.2.0:

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

NRF 23.2.0 Release

Updated the following sections with the details of NRF release 23.2.0:

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

NSSF 23.2.0 Release

Updated the following sections with the details of NSSF release 23.2.0:

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

Common Services Resolved Bugs

Updated the following sections with the details of Common Services Resolved Bugs for release 23.2.x:

- Egress Gateway Resolved Bugs
- Ingress Gateway Resolved Bugs
- Alternate Route Service Resolved Bugs
- ATS Resolved Bugs

Common Services Known Bugs

Updated the following sections with the details of Common Services Known Bugs release 23.2.x:

- Egress Gateway Known Bugs
- Ingress Gateway Known Bugs

- Alternate Route Service Known Bugs
- ATS Known Bugs

1 Introduction

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

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

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

2
Feature Descriptions

This chapter provides a summary of new features and updates to the existing features for network functions released in Cloud Native Core release 2.23.2.

2.1 Automated Testing Suite (ATS) Framework

Release 23.2.0

Oracle Communications Cloud Native Core, Automated Test Suite (ATS) framework 23.2.0 has been updated with the following enhancement:

- **ATS Tagging Support**: This feature allows you to run the feature files after filtering features and scenarios based on tags. For more information, see *"ATS Tagging Support"* in *Oracle Communications Cloud Native Core, Automated Testing Suite Guide*.

2.2 Binding Support Function (BSF)

Release 23.2.4

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

Release 23.2.3

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

Release 23.2.2

Oracle Communications Cloud Native Core, Binding Support Function (BSF) 23.2.2 has been updated with the following enhancement:

- **Enhancements to Audit Configurations**: Audit Service configurations in BSF is enhanced with addition of a new parameter "Minimum Audit Attempts" to BSF Management Service and options to configure Audit Service as well as Audit Schedule Data using CNC Console. These enhanced configurations resolve the issues related to identification and deletion of stale records by Audit Service. For more information, see "Configuring Binding Support Function" section in *Oracle Communications Cloud Native Core, Binding Support Function User Guide*.

Release 23.2.1

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

Release 23.2.0

Oracle Communications Cloud Native Core, Binding Support Function (BSF) 23.2.0 has been updated with the following enhancements:

- **Monitoring Availability of SCPs using SCP Health Check APIs**: BSF supports determining the availability and reachability status of all SCPs irrespective of the configuration types. It periodically determines the status of all SCPs. This monitoring is done at Egress Gateway microservice to ensure that the traffic is routed directly to the

healthy peers. This enhancement avoids routing or rerouting towards unhealthy peers minimizing the latency time. For more information about the feature, see "*Monitoring the Availability of SCP using HTTP2 OPTIONS*" section in *Oracle Communications Cloud Native Core, Binding Support Function User Guide*.

- **Supports 3gpp-Sbi-Correlation-Info Header**: BSF as a service consumer or as a service producer supports the forwarding or generation of 3gpp-Sbi-Correlation-Info header with UE identifier. This feature enables BSF to identify the UE related to the HTTP request or response of a specific subscriber. For more information about the feature, see "*Supports 3gpp-Sbi-Correlation-Info Header*" section in *Oracle Communications Cloud Native Core, Binding Support Function User Guide*.

2.3 Continuous Delivery Control Server (CDCS)

Oracle Communications CD Control Server (CDCS) 23.2.x has been updated with the following enhancements:

Release 23.2.2

Oracle Communications CD Control Server (CDCS) 23.2.2 has been updated with the following enhancements:

- **Support for Oracle Linux updates**: 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, and 23.2.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*.

For more detailed information about the features released in CDCS 23.2.2, see *Oracle Communications CD Control Server User Guide*.

Release 23.2.1

Oracle Communications CD Control Server (CDCS) 23.2.1 has been updated with the following enhancements:

- **Support for Oracle Linux updates**: 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, and 23.2.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*.

For more detailed information about the features released in CDCS 23.2.1, see *Oracle Communications CD Control Server User Guide*.

Release 23.2.0

Oracle Communications CD Control Server (CDCS) 23.2.0 has been updated with the following enhancements:

- **Supports Active and Standby CDCS Pair:** CDCS adds the ability to configure CDCS instances as Active and Standby pairs. When two CDCS instances are configured one in an active configuration and another in a Standby configuration, it ensures that lifecycle automation can be performed at all managed sites at any time. **Configure Mate CDCS** command is used to configure an Active and Standby CDCS pair. For more information about configuring Active and Standby pairs, see the "Configuring an Active and Standby CDCS Pair" section in *Oracle Communications CD Control Server User Guide*.
- **NF Configuration Change:** CDCS adds the ability to change the deployment configuration of an installed NF without upgrading the underlying software. **NF Config Change** command is used to change the configuration of an installed NF. For more information about NF configuration change, see the "Changing NF Configuration" section in *Oracle Communications CD Control Server User Guide*.
- **CDCS Enhancements:**
  - Supports installation and upgrade for CNE releases from 22.4.2, 23.1.x, and 23.2.0. The supported release versions are displayed as an option when running the **Upgrade OCCNE, Create New Production Site,** and **Create New Staging Site** commands.
  - Supports an option to specify a custom timeout that is added to the **Rollback NF Upgrade** command. In case, if your NF requires a longer timeout when rolling back a release, this field must be changed from the default five minutes to the value as recommended by the NF. This is applicable for releases 22.4.2, 23.1.x, and 23.2.0. For more detailed information about the features released in CDCS 23.2.0, see *Oracle Communications CD Control Server User Guide*.

2.4 Cloud Native Configuration Console (CNC Console)

Release 23.2.2

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

Release 23.2.1

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

Release 23.2.0

Oracle Communications Cloud Native Configuration Console (CNC Console) 23.2.0 has been updated with the following enhancements:

- **Remove Database Dependency from Agent CNC Console**: CNC Console has removed database dependency from Agent CNC Console (A-CNCC) to reduce resource requirements. This is achieved by eliminating the dependency on the cmservice, which in turn eliminates the dependency on the database. This has led to the elimination of cnDBTier profile2 and a reduction in resource usage by the Console. For more information, see *Oracle Communications Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide*.
- **Adapt the NF Controlled Shutdown GUI for all NFs**: New Console GUI screen templates have been added to enable NFs to render NF scoring data. This data helps operators to identify the NF instances that are causing NF failure in the GR setup and shutdown those instances till the issue is resolved. The screen templates can be used by NFs to develop backend APIs and use this functionality.
- **Configure Kubernetes Network Policies**: CNC Console has implemented the Network policies framework to enable the user to specify how a pod communicates with network entities. It enables Console to create pod-level rules needed for CNC Console data flows, to manage Ingress and Egress traffic, and allow traffic between CNC Console pods. For

more information, see *Oracle Communications Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide*.

- **NF Versions Supported by CNC Console**: The following NF versions are supported in this release:
  - SCP - 23.2.x
  - NRF - 23.2.x
  - UDR - 23.2.x
  - POLICY - 23.1.x
  - BSF - 23.1.x
  - SEPP - 23.2.x
  - NSSF - 23.2.x
  - DD - 23.2.x
  - NWDAF - 23.2.x
  - PROVGW - 23.2.x

2.5 Cloud Native Core cnDBTier

Release 23.2.5

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

Release 23.2.4

Oracle Communications Cloud Native Core, cnDBTier (cnDBTier) 23.2.4 has been updated with the following 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 *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*.
  Consideration:

  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 on 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 on a cnDBTier version that is higher than the version on the bad site.
    * The good site runs on 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
- **TLS Support for Georeplication**: TLS feature is disabled by default in this release.

Release 23.2.3

Oracle Communications Cloud Native Core, cnDBTier (cnDBTier) 23.2.3 has been updated with the following enhancements:

- **TLS Support for Georeplication**: With this feature, cnDBTier automates the process of configuring TLS for georeplication between cnDBTier sites. On enabling this feature, the replication SQL pod uses the certificates provided or configured to establish an encrypted connection for georeplication. This ensures that the replication data transfer is secure. For more information about this feature, see *Oracle Communications Cloud Native Core, cnDBTier User Guide* and *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*.
  Considerations: If you are enabling TLS for the replication channels in this release, be informed about the following conditions:
  - You can't rollback from 23.2.3 to previous releases.
  - You can't upgrade from 23.2.3 to 23.3.x or 23.4.x. However, cnDBTier plans to resolve this upgrade restriction in a future release.
  - You can't scale the nodes or replication channels.
  - You can't add or remove replication channels.

Release 23.2.2

Oracle Communications Cloud Native Core, cnDBTier (cnDBTier) 23.2.2 has been updated with the following enhancements:

- **Support for New Version of Spring Boot**: Spring Boot is upgraded to 2.7.15 in this release.

Release 23.2.1

Oracle Communications Cloud Native Core, cnDBTier (cnDBTier) 23.2.1 has been updated with the following enhancements:

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

Release 23.2.0

Oracle Communications Cloud Native Core, cnDBTier 23.2.0 has been updated with the following enhancements:

- **Database Backup Encryption and Secure Transfer**: cnDBTier backups contain sensitive subscriber data. These backups are transferred to remote servers and sites for performing fault recovery. With this release, cnDBTier provides an option to encrypt and decrypt the on-demand or periodic backups at the cluster level. Additionally, cnDBTier provides the functionality to securely transfer the backups stored in the data nodes to remote sites using

Secure File Transfer Protocol (SFTP). For more information on this feature, see *Oracle Communications Cloud Native Core, cnDBTier User Guide*.

- **Replacing SQL Commands in cnDBTier Procedures with REST APIs (Extension)**: In the previous release, cnDBTier replaced SQL commands in cnDBTier procedures with REST APIs. In this release, cnDBTier has additionally introduced the following REST APIs to replace SQL commands in cnDBTier procedures. This restricts the access to MySQL credentials and avoids the manual errors of breaking the replication between other remote sites.
  - REST API to retrieve cnDBTier and NDB version.
  - REST API to retrieve the real time status of cnDBTier replication service.
  - REST API to retrieve the number of databases, tables, and row count of each table in cnDBTier.

  For more information about these REST APIs, see the "*cnDBTier APIs*" section in *Oracle Communications Cloud Native Core, cnDBTier User Guide*.
- **PVC Health Monitoring**: Before implementing this feature, to identify any PVC issues, you must wait for the MySQL Cluster processes to log an error. With this feature, cnDBTier provides options to monitor the health of PVCs that are mounted on cnDBTier pods. For more information about this feature, see Oracle Communications Cloud Native Core, cnDBTier User Guide.
- **MySQL Support for Multi Threaded Applier (MTA) Feature**: This feature provides the functionality to run independent binlog transactions parallelly at a replica, thereby increasing the peak replication throughput. MySQL 8.0.33 supports the MTA feature. As cnDBTier 23.2.0 comes with MySQL 8.0.33, NDB replication is modified to support the use of generic MySQL Server MTA mechanism. This feature is a code level enhancement in NDB which is enabled by default. It can be disabled from cnDBTier through additional configuration. For more information, see *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*.
- **Support to Enable Query Log on SQL Pods**: With this release, cnDBTier provides support to enable query logging on selected SQL pods to trace SQL activities. For more information, see *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*.
- **Recovery Script for Database Resync**: Starting with this release, cnDBTier provides the dbtrecover recovery script as part of the CSAR package to perform DB resync in georeplication clusters.
- **Support to Kyverno Policies**: Kubernetes 1.25.x has discontinued the support for Pod Security Policy (PSP). As CNE 23.2.x comes with Kubernetes 1.25.x, it provides Kyverno as a replacement for PSP. Therefore, with this release, cnDBTier supports Kyverno policies. For more information, see the "Creating Namespace" and "Upgrading cnDBTier" sections in *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*.
- **Support for New Version of MySQL Cluster Software**: The Oracle MySQL Cluster Database software is upgraded to 8.0.33 in this release.
- **MySQL Support for Multi Threaded Applier (MTA) Feature**: This feature implementation has certain issues and has to be manually disabled before an installation or upgrade. Therefore, before performing an installation or upgrade, ensure that you follow the updated installation or upgrade procedure in 23.3.0 *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide* to disable the MTA feature .

2.6 Cloud Native Environment (CNE)

> **Note:**
>
> The procedure to update OpenStack credentials is revised in the 23.2.6 User Guide. If you are updating OpenStack credentials on other versions of 23.2.x, refer to the latest procedure from 23.2.6 *Oracle Communications Cloud Native Core, Cloud Native Environment User Guide*.

Release 23.2.6

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

Release 23.2.5

Oracle Communications Cloud Native Core, Cloud Native Environment (CNE) 23.2.5 has been updated with the following enhancements:

> **Note:**
>
> The following feature was introduced in 23.2.4 which is an installation-only patch. Therefore, if you are upgrading to 23.2.5, be informed about the following feature that is already in place.

- **New Versions of Common Services:** The following OpenSearch services are upgraded in 23.2.4:
  - Oracle OpenSearch - 2.3.0
  - Oracle OpenSearch Dashboard - 2.3.0
  - Fluentd OpenSearch - 1.16

  These upgrades provide number of new features offered by OpenSearch. For example, Fluent Bit is replaced with Fluentd OpenSearch. That is, log forwarding mechanism is changed from fluent-bit to fluentd-openSearch. The other changes in the OpenSearch stack are as follows:
  - There are five OpenSearch data nodes created by default.
  - Upgrade from 23.1.x to 23.2.5 has Elastic Search to store old index data and OpenSearch to ingest new data.
  - Elastic Search and Kibana are removed when upgrading from 23.1.x to 23.2.x.
  - Upgrade from 23.2.1 and 23.2.3 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 the collection of these metrics.

To get the complete list of third party services and their versions, refer to the `dependencies_23.2.5.tgz` file provided as part of the software delivery package.

Release 23.2.4

Oracle Communications Cloud Native Core, Cloud Native Environment (CNE) 23.2.4 has been updated with the following enhancements:

- **New Versions of Common Services:** The following OpenSearch services are upgraded in this release:
  - Oracle OpenSearch - 2.3.0
  - Oracle OpenSearch Dashboard - 2.3.0
  - Fluentd OpenSearch - 1.16

  These upgrades provide number of new features offered by OpenSearch. For example, Fluent Bit is replaced with Fluentd OpenSearch. That is, log forwarding mechanism is changed from fluent-bit to fluentd-openSearch. 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 the collection of these metrics.

  To get the complete list of third party services and their versions, refer to the `dependencies_23.2.4.tgz` file provided as part of the software delivery package.

Release 23.2.3

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

Release 23.2.1

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

Release 23.2.0

Oracle Communications Cloud Native Core, Cloud Native Environment (CNE) 23.2.0 has been updated with the following enhancements:

- **Automated Addition and Removal of Worker Node for Bare Metal**: With this release, CNE provides automated procedures to add a new worker node to a Bare Metal deployment and remove a worker node from a Bare Metal deployment. These procedures also provide persistent logging functionality. For more information about these procedures, see *Oracle Communications Cloud Native Core, Cloud Native Environment User Guide*.
- **Local DNS**: Local DNS allows the pods and services running inside the CNE cluster to connect with the ones running outside the CNE cluster using core DNS. That is, when Local DNS is enabled, CNE routes the connection to external hosts through core DNS rather than the nameservers on the Bastion Hosts. This feature enables the following capabilities:
  - It allows you to add entries directly to the CNE DNS subsystem and remove the entries when required. These entries can be used to identify and locate NFs located outside the CNE cluster.
  - It allows you to disable access to DNS nameservers outside the CNE cluster.

For information about this feature, see *Oracle Communications Cloud Native Core, Cloud Native Core User Guide*.

- **End of Life for PSP**: Kubernetes 1.25.x has discontinued the support for Pod Security Policies (PSP). As CNE 23.2.0 comes with Kubernetes 1.25.x, CNE doesn't support PSP. CNE has adopted a new framework Kyverno in place of PSP. Kyverno provides security policies for CNE clusters and all PSP-based access or security policies are upgraded with Kyverno. For more information on this framework, see *Oracle Communications Cloud Native Core, Cloud Native Environment User Guide* and *Oracle Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide*.
- **New Versions of Common Services**: The following common services are upgraded in this release:
  - Helm - 3.10.3
  - Kubernetes - 1.25.6
  - containerd - 1.6.15
  - Calico - 3.23.3
  - MetalLB - 0.13.7
  - Prometheus - 2.39.1
  - Grafana - 9.1.7
  - Jaeger - 1.39.0
  - Istio - 1.15.3
  - Kyverno - 1.9.0
  - cert-manager - 1.10.0

  You can find the complete list of third party services and their versions in the `dependencies_23.2.0.tgz` file provided as part of the software delivery package.

Operations Services Overlay (OSO)

Oracle Communications Operations Services Overlay (OSO) 23.2.0 has been updated with the following enhancements:

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

- NGINX ingress controller - 1.5.1
- Alert Manager - 0.25.0

For more information about these uplifts, see *Oracle Communications Operations Services Overlay Installation and Upgrade Guide*.

2.7 Network Exposure Function (NEF)

Release 23.2.1

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

Release 23.2.0

Oracle Communications Cloud Native Core, Network Exposure Function (NEF) 23.2.0 has been updated with the following enhancements:

The following three functionalities are achieved by utilizing the 3GPP-defined monitoring events based on the monitoring type. The detection of these events relies on the event reporting parameters received in the monitoring event subscription request:

- **Support for PDU Session Status Event**: This feature enables NEF to deliver PDU Session status information to AFs. 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 UE Reachability Event**: This feature enables NEF to deliver UE Reachability information to AFs. 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 Loss of Connectivity Event**: This feature enables NEF to deliver Loss of Connectivity information to AFs. 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*.

2.8 Network Repository Function (NRF)

Release 23.2.3

Oracle Communications Cloud Native Core, Network Repository Functions (NRF) 23.2.3 has been updated with the following enhancement:

- Supports Service Level Priority with 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 same service name after processing the discovery query.
  For more information about the feature, see "Extended Preferred Locality Priority Handling" in *Oracle Communications Cloud Native Core, Network Repository Function User Guide*.

Release 23.2.2

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

Release 23.2.1

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

Release 23.2.0

Oracle Communications Cloud Native Core, Network Repository Functions (NRF) 23.2.0 has been updated with the following enhancements:

- **User-Agent Header for Outgoing Requests**: NRF supports the addition of User-Agent header for outgoing messages such as NFStatusNotify and SLF query requests. If the User-Agent header value is configured, then NRF adds the User-Agent header with the configured value to the mentioned outgoing messages. For more information about the feature, see "*User-Agent Header for Outgoing Requests*" in *Oracle Communications Cloud Native Core, Network Repository Function User Guide*.
- **Network Slice Specific Metrics**: NRF allows to measure the number of requests and responses for various service operation per network slice. These slices are identified by Network Slice Instances (NSIs) and Single Network Slice Selection Assistance Information (SNSSAI). This measurement is performed using the metrics. For more information about

the feature, see "*Network Slice Specific Metrics*" in *Oracle Communications Cloud Native Core, Network Repository Function User Guide*.

- **Kubernetes Tolerations**: NRF allows to configure tolerations. The tolerations allow scheduling the pods onto nodes with matching taints but do not guarantee scheduling. When a taint is assigned by Kubernetes configurations, it repels all the pods except those that have a matching toleration for that taint. For more information about the feature, see "*Tolerations*" in *Oracle Communications Cloud Native Core, Network Repository Function User Guide*.
- **Enhancement for Auditing the Availability of NRF Tables**: NRF detects any inconsistency in the system at an early stage of upgrade and reports the same based on the NRF tables validation. The validations are done during the preupgrade and postupgrade. For more information about the feature, see "*Audit NRF Database Tables*" in *Oracle Communications Cloud Native Core, Network Repository Function User Guide*.
- **Controlled Shutdown of NRF**: NRF supports isolating an NRF from the current network at a particular site. This isolation helps to perform any maintenance activities or recovery procedures as required without uninstalling the NRF at the particular site. For more information about the feature, see "*Controlled Shutdown of NRF*" in *Oracle Communications Cloud Native Core, Network Repository Function User Guide*.
- **Monitoring Availability of SCPs using SCP Health Check APIs**: NRF supports determining the availability and reachability status of all SCPs irrespective of the configuration types. It periodically determines the status of all SCPs. This monitoring is done at Egress Gateway microservice to ensure that the traffic is routed directly to the healthy peers. This enhancement avoids routing or rerouting towards unhealthy peers minimizing the latency time. For more information about the feature, see "*Monitoring the Availability of SCP using HTTP2 OPTIONS*" in *Oracle Communications Cloud Native Core, Network Repository Function User Guide*.
- **CCA Header validation in NRF for Access Token Service Operation:** The Client credentials assertion (CCA) is a token signed by the Consumer NF. It enables NRF to authenticate the Consumer NF which includes the signed token in Access Token service request. CCA header contains the Consumer NF's NfInstanceId that gets checked against the certificate by the NRF. The CCA also includes a timestamp as the basis for the restriction of its lifetime. For more information about the feature, see "*CCA Header validation in NRF for Access Token Service Operation*" in *Oracle Communications Cloud Native Core, Network Repository Function User Guide*.
- **Aspen Service Mesh with New Resources**: NRF supports additional two new resources in ASM Custom Resource Definitions (CRDs), Request Authentication and Policy Authorization. Also, Support for additional new attributes is added to existing ASM CRDs. For more information about the feature, see "*Configuring NRF to Support ASM*" in *Oracle Communications Cloud Native Core, Network Repository Function Installation, Upgrade, and Fault Recovery Guide*.
- **Enhancement of NRF Fault Recovery on Recovering NRF from Old Backup**: NRF supports fault recovery using the old backup taken from NRF. For more information about the feature, see "*Fault Recovery*" in *Oracle Communications Cloud Native Core, Network Repository Function Installation, Upgrade, and Fault Recovery Guide*.

2.9 Network Slice Selection Function (NSSF)

Release 23.2.0

Oracle Communications Cloud Native Core, Network Slice Selection Function (NSSF) 23.2.0 has been updated with the following enhancements:

- **Monitoring the Availability of SCPs using SCP Health APIs**: With this feature, NSSF determines the availability and reachability status of all SCPs irrespective of the configuration types. This feature is an enhancement to the existing SBI routing functionality. Egress Gateway microservice interacts with SCP on their health API endpoints using the HTTP2 OPTIONS method. It monitors the health of configured SCP peers to ensure that the traffic is routed directly to the healthy peers. This enhancement avoids routing or rerouting towards unhealthy peers, thus minimizing the latency time. For more information about the feature, see "*Monitoring the Availability of SCPs using SCP Health APIs*" in *Oracle Communications Cloud Native Core, Network Slice Selection Function User Guide*.
- **Validation of WWW-Authenticate Response Header 4xx with NSSF**: When access-token validation is enabled, NSSF performs access-token validation of the access-token that comes with service requests to it. With this enhancement, NSSF has added supports 3GPP specified 4XX application error codes for these access token checks. For more information, see *Oracle Communications Cloud Native Core, Network Slice Selection Function User Guide*.
- **Deleting Subscription on 404 SUBSCRIPITON_NOT_FOUND Response from AMF**: On setting the ***deleteOnSubscriptionNotFound*** parameter as **true** in the custom_values.yaml file, NSSF automatically deletes subscriptions upon receiving a ***404 SUBSCRIPTION_NOT_FOUND*** response from AMF for a subscription notification. However, by setting **deleteOnSubscriptionNotFound** to false, NSSF retains the subscription even after encountering the ***404 SUBSCRIPITON_NOT_FOUND*** response. For more information, see *Oracle Communications Cloud Native Core, Network Slice Selection Function User Guide*.

2.10 Policy

Release 23.2.8

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

Release 23.2.7

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

Release 23.2.6

Oracle Communications Cloud Native Core, Converged Policy 23.2.6 has been updated with the following enhancements:

- **Session Retry Enhancement at Egress Gateway**: With this enhancement, the *sbiroutingerrorcriteriasets* parameter has been enhanced to include the error cause. As a result, when Egress Gateway receives HTTP error response based on the matching *errorcriteria*, there is a retry of failed request through an alternate SCP based on the defined *erroractionset*. For more information, see *Support for Session Retry and Alternate Route Service* section in *Oracle Communications Cloud Native Core, Converged Policy User Guide.*
- **Support for Binding Header and Routing Binding Header in N1N2Transfer**: This feature enables the user to configure binding header, routing binding header, and the discovery header for N1N2Transfer requests. For more details, see "Support for 3GPP NF Sets and Binding Headers" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide.*
- **PDS Handling Subscription Failure from UDR**: This feature adds advanced settings keys in PDS Settings page on CNC Console. In case of UDR subscription failure with subscribeToNotify flag enabled, the user can configure these newly added keys to enable

PCF to reattempt sending the subscription request toward UDR service on next SM update. For more details, see "Support for Query on Update and Subscription to UDR" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide.*

Release 23.2.5

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

Release 23.2.4

Oracle Communications Cloud Native Core, Converged Policy 23.2.4 has been updated with the following enhancements:

- **PCF to include Service Name in Binding Header towards UDR, CHF, BSF, and AMF**: PCF as a consumer sends binding headers to producer NFs such as UDR, CHF, BSF, and AMF during explicit or implicit subscription. When *Send PCF Service Name in Binding Header* parameter is enabled, the binding header includes servname along with other details such as `nfinst` and `nfset`. When a notification request from UDR, CHF, BSF, or AMF to PCF fails, the producer NFs can use the servname in the binding header to select an alternate PCF. For more information, see "Support for 3GPP NF Sets and Binding Headers" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide.*
- **IPv6 enablement in Policy**: Two new parameters, *global.isIpvSixSetup* and *diam-gateway.envSupportedIpAddressType* have been added to enable and configure IPv6 in Policy.For more information, see "Configuration Parameters for IPv6" section in *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide*.
- **Binding Stale Session Cleanup**: Policy enables Binding service to trigger remote or local stale session clean up request towards SM service when the number of SM sessions per DNN exceeds the configured *Max sessions per DNN* value. The binding flag *Max Session Cleanup Mode* used by the Binding service controls the deletion of stale binding sessions. For more information, see "Binding Service" feature section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.

Release 23.2.2

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

Release 23.2.1

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

Release 23.2.0

Oracle Communications Cloud Native Core, Converged Policy 23.2.0 has been updated with the following enhancements:

- **Adding Subscription-ID AVPs to STR Messages**: As part of the Final Spending Limit Report Request (SLR) procedure, PCRF sends a Session Termination Request (STR) to Online Charging System (OCS) through PDS and Diam-Connector to unsubscribe from all the Policy Counters belonging to the Diameter session and terminate the session. Adding Subscription-ID AVPs allow OCS to associate the STR with the SLR and close the session. For more information, see "*Adding Subscription-ID AVPs to STR messages*" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.
- **Support for Subscriber Notification Using SMPP**: Policy supports sending subscriber notification (SMS alerts regarding Quota management or usage reporting and activation/ deactivation of services) to subscribers through SMPP (Short Message Peer-to-Peer)

protocol. This feature enables transfer of short messages between External Short Message Entities (ESME) and Message Centres (MC). For more information, see "*Support for Subscriber Notification Using SMPP*" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.

- **Support for Query on Update and Subscription to UDR**: Policy supports querying the UDR for user data when a Policy Service (SM Service, AM Service, or UE Policy Service) receives an update request. This feature enables sending the GET request along with POST Subscribe to UDR when processing an Update request with `queryOnUpdate` and `subscribeToNotify` flags enabled. For more information, see "*Support for Query on Update and Subscription to UDR*" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide.*
- **Support for Auto Enrolment of Subscribers**: Policy supports auto-provisioning of the subscribers at UDR by applying dynamic quota when the subscriber profile is not present in UDR. For more information, see "*Support for AutoEnrolment of Subscribers*" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide.*
- **Support for Presence Reporting Area**: PCF supports the Presence Reporting Area (PRA) functionality to comply with the 3GPP standards. Policy supports PRA functionality for SM Service, AM Service, and UE Policy Service. For more information, see "*Support for Presence Reporting Area*" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.
- **Handling Install and Remove Conflict for Same Rule**: In certain policies, install/update and remove actions are applied for the same rule - which can be either a session rule or a PCC rule. This feature resolves conflicts between INSTALL and REMOVE actions on the same PCC/Session Rules when the remove action is Remove ALL (ALL, Predefined, Dynamic, Conditioned, non-conditioned) in the policy project. The feature uses `Install/Remove Rule Conflicts Strategy` parameter under PCF Session Management service configurations to resolve the conflict. For more information, see "*Handling Install and Remove Conflict for Same Rule*" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.
- **Usage Monitoring on Gx Interface**:
  Cloud Native 4G Policy implements Usage Monitoring or Quota Management using the combination of PCRF Core and Usage Monitoring. These two microservices have their respective policy engines and thus separate policy projects. Each of the two microservices (along with their respective policies) has the following functions with respect to Quota Management:
  - PCRF Core - Controls PCC and/or Session Rules and Charging Description
  - Usage Monitoring - Controls the Quota Selection, Accumulation and Grant

  For more information, see "*Usage Monitoring on Gx Interface*" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.
- **Monitoring Availability of SCPs using SCP Health Check APIs**: PCF delivers UE policy to the UE in several MANAGE UE POLICY COMMAND messages as fragments. Using the PCF UE blockly's UE policy is installed with fragmentation. This feature allows UE Policy installation with fragmentation, by providing URSP data type and URSP List data type: as a column in the policy table. For more information about the feature, see "*UE Policy Improvements*" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.
- **Remote State Subscriber Variable**: Subscriber State variables hold the intermediate state of the policy evaluation. The state variables are defined by the policy writer that can be set within a policy action to be used at a later time during policy rule execution. The remote subscriber state variable persists in UDR. The PCF interfaces with User Data Repository (UDR) to receive subscriber-related Policies for User Equipment(UE). PCF

communicates with UDR to receive these attributes which are used in the evaluation of Policies. For more information about the feature, see "*Subscriber State Variables in Policy*" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.

- **Support for Diameter Error Codes**: Policy supports diameter error codes for RX and BSF. For more information about the feature, see "*Diameter Error Codes*" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.
- **Error Mapping for CHF Interface**: Policy supports handling of the errors received from CHF interface as well as errors to be responded to CHF notification. For more information about the feature, see "*HTTP Error Codes*" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.
- **Error Mapping for UDR Interface**: Policy supports handling of the errors received from CHF interface as well as errors to be responded to UDR notification. For more information about the feature, see "*HTTP Error Codes*" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.
- **Error Mapping for AM Interface**: Policy supports error cause along with HTTP error codes while sending an error to the AM interface. It also supports handling of errors received for notification. For more information about the feature, see "*HTTP Error Codes*" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.
- **Error Mapping for SM Interface**: Policy supports error cause along with HTTP error codes while sending an error to the SM interface. It also supports handling of errors received for notification. For more information about the feature, see "*HTTP Error Codes*" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.
- **Error Mapping for UE Interface**: Policy supports error cause along with HTTP error codes while sending an error to the AM interface for UE Policy. It also supports handling of errors received for notification. For more information about the feature, see "*HTTP Error Codes*" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.
- **Error Mapping for NRF Interface**: Policy supports handling of the errors received from NRF interface as well as errors to be responded to NRF notification. For more information about the feature, see "*HTTP Error Codes*" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.
- **Support for Data Compression**: Policy supports data compression to reduce the data size and hence the storage used by database. It can also be used to improve the communication latency between application and database when compression is performed at the application level. It is supported for SM, Binding, and PDS services. For more information about the feature, see "*Data Compressions*" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.

2.11 Service Communication Proxy (SCP)

Release 23.2.3

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

Release 23.2.2

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

Release 23.2.1

Oracle Communications Cloud Native Core, Service Communication Proxy (SCP) 23.2.1 has been updated with the following enhancements:

- **Enhanced NF Status Processing**: This is an enhancement to the Mode 2 routing option of SCP to consider all NFs for routing that are configured using the `suspendedStateRouting` REST API parameter to route the message request. For more information, see "Enhanced NF Status Processing" in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.
- **Dual Stack Support**: This feature enables SCP to support deployment on Dual Stack with IPV4 preferred. For more information, see "Support for Kubernetes Resources" in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.
- **ASM Envoy Filter Configuration Enhancements**: This enhancement has introduced `cluster.service` and `type` fields for Envoy Filter CRD. For more information, see "ASM Configuration" in *Oracle Communications Cloud Native Core, Service Communication Proxy Installation, Upgrade, and Fault Recovery Guide*.

Release 23.2.0

Oracle Communications Cloud Native Core, Service Communication Proxy (SCP) 23.2.0 has been updated with the following enhancements:

- **Support for Default Notification Message Routing**: This feature enables SCP to create routing rules in the callback URI of the default notification subscription to route the 5G SBI messages after learning the 5G topology from NRF through NF status notifications. For more information, see *"Support for Default Notification Routing"* in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.
- **Support for 5G SBI Message Correlation using the 3gpp-Sbi-Correlation-Info Header**: This feature enables SCP with correlation data, such as User Equipment (UE) identity, that an operator uses in various offline network management, performance analysis, and troubleshooting tools and applications to identify the requests and responses related to a specific subscriber. For more information, see *"Support for 5G SBI Message Correlation using the 3gpp-Sbi-Correlation-Info Header"* in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.
- **Support for the ClientCredentials Assertion Header**: This feature enables the NRF or the producer NF to authenticate the consumer NF when using indirect communication through SCP. For more information, see *"Support for the ClientCredentials Assertion Header"* in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.
- **Support for Network Policies**: This feature enables SCP to create pod-level rules that control communication between the cluster's pods and services and determine which pods and services can access one another inside the cluster. For more information, see *"Network Policies"* in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.
- **SCP Health Check API**: The SCP Health Check Application Programming Interface (API) feature enables consumer NFs to determine the health status of SCP by sending health query requests to SCP before forwarding any SBI message request to SCP. For more information, see *"SCP Health Check API"* in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.
- **Verbose Logging for SCP**: This feature defines a common log format to include required information to enhance the debugging process for WARN and ERROR logs. Using this log format, ERROR and WARN level logs are modified to standardize the log format, add more details, and enhance readability. For more information, see *"Verbose Logging for SCP"* in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.
- **Pod Overload Control Enhancement**: This enhancement enables SCP to throttle only ingress 5G SBI message requests based on Pending Transactions for which responses

from producer NFs are awaited by SCP. For more information, see *"Pod Overload Control"* in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.

- **5G SBI Message Failure Handling using Server Header Enhancement**: The 5G SBI Message Failure Handling functionality is enhanced so that SCP forwards the last or latest error response received from producer NFs to consumer NFs, and server header content is populated with the details of the producer NF from which the error response is received. For more information, see *"Enhanced 5G SBI Message Failure Handling"* in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.
- **Support for OAuth2.0**: This feature enables SCP to support OAuth2.0 (Open Authorization) access tokens in 5G indirect communication models such as Model C and Model D. SCP uses the access tokens received from consumer NFs and Network Repository Function (NRF) and forward Service Based Interface (SBI) message requests to the selected producer NFs. For more information, see *"Support for OAuth2.0"* in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.

2.12 Security Edge Protection Proxy (SEPP)

Release 23.2.2

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

Release 23.2.1

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

Release 23.2.0

Oracle Communications Cloud Native Core, Security Edge Protection Proxy (SEPP) 23.2.0 has been updated with the following enhancements:

- **Support for Cat 0 - SBI Message Schema Validation**: This feature supports stateless security countermeasures, which enhance the security measures of roaming partners by allowing only valid requests to be processed at SEPP. It performs checks to determine the validity of messages. This feature is designed to support the following:
  - Verifying the combination of request body and query parameters and compare it with the respective schema.
  - Routing of only valid SBI messages to egress or ingress the network.

  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*, and *"Cat-0 SBI Message Schema Validation"* section in *Oracle Communications Cloud Native Core, Security Edge Protection Proxy REST API Specification Guide*.
- **Support for Cat-3 Previous Location Check**: The feature is part of stateful security countermeasures, verifying that only authenticated User Equipment (UE) messages originating from the same location as the UE's authentication are allowed.
  The authentication status of a specific UE is obtained from the UDR in the home network, and this information is checked for every incoming message received by the Producer SEPP (P-SEPP). If the UE is successfully authenticated based on the UDR response, the message is allowed to pass through the P-SEPP. However, if the UE is not authenticated or if the location of the incoming message does not match the location registered in the UDR during the UE authentication process, the message is rejected and an error message, configurable by the user, is displayed. This feature is exclusively available on the P-SEPP.

For more information about the feature, see the *"Cat-3 Previous Location Check Feature"* section in *Oracle Communications Cloud Native Core, Security Edge Protection Proxy User Guide*, *"Cat-3 Previous Location Check"* 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*.

- **Supports Kubernetes 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. To control communication between the cluster's pods and services and to determine which pods and services can access one another inside the cluster, it creates pod-level rules.
  The Kubernetes Network Policies for SEPP provides namespace-level isolation for SEPP pods. The pods deployed within the SEPP can communicate with each other directly, while any other pods, whether inside or outside the namespace, must communicate through the gateways.

  For more information about the feature, see the *"Support for Network Policies"* section in *Oracle Communications Cloud Native Core, Security Edge Protection Proxy User Guide*, and *"Configuring Network Policies"* section in *Oracle Communications Cloud Native Core, Security Edge Protection Proxy Installation, Upgrade, and Fault Recovery Guide*.
- **Running ATS Test Cases on SUT with a Parameterized Approach**: 5G ATS framework is enhanced to add the capability of running Test Cases with the System Under Test (SUT) in a customer-specific production configuration. Additionally, SEPP is updated to support the parameterized architecture provided by 5G ATS. For more information about the feature, see *Oracle Communications Cloud Native Core Automated Testing Suite Guide*.
- **Validate the GZIP functionality for Message Copy Feature**: In previous releases, logs were not displayed in GZIP format for the Message Copy feature. With this release, Ingress and Egress Gateways support is enhanced to display the logs in the GZIP format for the Message Copy feature.

2.13 Unified Data Repository (UDR)

Release 23.2.2

Oracle Communications Cloud Native Core, Unified Data Repository (UDR) 23.2.2 has been updated with the following enhancement:

- **Suppress Notification**: This feature enables cnUDR to store the User-Agent header received in the POST request from cnPCRF in the subscription table. cnUDR compares the User-Agent header received during an update operation from cnPCRF with the stored User-Agent header, if the User-Agent header matches, then the notification is suppressed. The notification is sent if the User-Agent header does not match or if the there is no User-Agent header in the update request. For more information about the feature, see *"Suppress Notification"* section in *Oracle Communications Cloud Native Core, Unified Data Repository User Guide*.

Release 23.2.1

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

Release 23.2.0

Oracle Communications Cloud Native Core, Unified Data Repository (UDR) 23.2.0 has been updated with the following enhancements:

- **NF Scoring for a Site**: 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. For more information about the feature, see *"NF Scoring for a Site"* section in *Oracle Communications Cloud Native Core, Unified Data Repository User Guide*.
- **Converged Quota Support for Provisioning Interface**: In this feature 5G Policy and Charging Rules Function (PCRF) interacts with 5G UDR for both 4G and 5G data. The 5G PCRF must store the quota information under sm-data/umData and sm-data/umDataLimits. The data model is updated to support the storage of 4G policy data under sm-data/umData and sm-data/umDataLimits from VSA. For more information about the feature, see *"Converged Quota Support for Provisioning Interface"* section in *Oracle Communications Cloud Native Core, Unified Data Repository User Guide*.
- **Controlled Shutdown of an Instance Integration with CNC Console**: This feature enables CNC Console support to provide the partial or complete isolation of the site from the network so that the operator can perform necessary recovery procedures. For more information about the feature, see *"Controlled Shutdown of an Instance"* and *"Controlled Shutdown Configurations"* sections in *Oracle Communications Cloud Native Core, Unified Data Repository User Guide.*
- **Provision Gateway Auditor Enhancements**: Provision Gateway is enhanced to support monitoring APIs of Provision Gateway auditor in SLF mode through CNC Console to show the current status of auditor process. Alerts are also added for Persistent Volume Claim (PVC) monitoring of Auditor service. For more information about the feature, see *"Using Auditor Service and Auditor Service Status"* in *Oracle Communications Cloud Native Core, Provisioning Gateway Guide*.
- **UDR and Provision Gateway Configuration API Enhancements**: UDR and Provision Gateway configuration APIs are enhanced to do a strict validation of input and modify the return codes.

3
Media and Documentation

3.1 Media Pack

This section lists the media package for Oracle Communications Cloud Native Core 2.23.2. 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 2.23.2

Description	NF Version	ATS Version	Upgrade Supported
Oracle Communications Cloud Native Core, Binding Support Function (BSF)	23.2.4	23.2.3	BSF 23.2.4 supports fresh installation and upgrade from 22.4.x, 23.1.x, and 23.2.x. For more information, see *Oracle Communications Cloud Native Core, Binding Support Function Installation, Upgrade, and Fault Recovery Guide.*
Oracle Communications Cloud Native Core, Binding Support Function (BSF)	23.2.3	23.2.3	BSF 23.2.3 supports fresh installation and upgrade from 22.4.x, 23.1.x, and 23.2.x. For more information, see *Oracle Communications Cloud Native Core, Binding Support Function Installation, Upgrade, and Fault Recovery Guide.*
Oracle Communications Cloud Native Core, Binding Support Function (BSF)	23.2.2	23.2.2	BSF 23.2.2 supports fresh installation and upgrade from 22.4.x, 23.1.x, and 23.2.x. For more information, see *Oracle Communications Cloud Native Core, Binding Support Function Installation, Upgrade, and Fault Recovery Guide.*

Table 3-1 (Cont.) Media Pack Contents for Oracle Communications Cloud Native Core 2.23.2

Description	NF Version	ATS Version	Upgrade Supported
Oracle Communications Cloud Native Core, Binding Support Function (BSF)	23.2.1	23.2.1	BSF 23.2.1 supports fresh installation and upgrade from 22.4.x, 23.1.x, and 23.2.0. For more information, see *Oracle Communications Cloud Native Core, Binding Support Function Installation, Upgrade, and Fault Recovery Guide.*
Oracle Communications Cloud Native Core, Binding Support Function (BSF)	23.2.0	23.2.0	BSF 23.2.0 supports fresh installation and upgrade from 23.1.x and 22.4.x. For more information, see *Oracle Communications Cloud Native Core, Binding Support Function Installation, Upgrade, and Fault Recovery Guide.*
Oracle Communications Cloud Native Configuration Console (CNC Console)	23.2.2	NA	CNC Console 23.2.2 supports fresh installation and upgrade from 22.4.x, 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 Configuration Console (CNC Console)	23.2.1	NA	CNC Console 23.2.1 supports fresh installation and upgrade from 22.4.x, 23.1.x, and 23.2.0. For more information, see *Oracle Communications Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide.*
Oracle Communications Cloud Native Configuration Console (CNC Console)	23.2.0	NA	CNC Console 23.2.0 supports fresh installation and upgrade from 22.4.x and 23.1.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)	23.2.6	NA	CNE 23.2.6 supports fresh installation and upgrade from 23.1.x and 23.2.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)	23.2.5	NA	CNE 23.2.5 supports fresh installation and upgrade from 23.1.x and 23.2.x. For more information, see *Oracle Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide*.

Table 3-1 (Cont.) Media Pack Contents for Oracle Communications Cloud Native Core 2.23.2

Description	NF Version	ATS Version	Upgrade Supported
Oracle Communications Cloud Native Core, Cloud Native Environment (CNE)	23.2.4	NA	CNE 23.2.4 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)	23.2.3	NA	CNE 23.2.3 supports fresh installation and upgrade from 23.1.x and 23.2.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)	23.2.1	NA	CNE 23.2.1 supports fresh installation and upgrade from 23.1.x and 23.2.0. 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)	23.2.0	NA	CNE 23.2.0 supports fresh installation and upgrade from 23.1.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)	23.2.0	NA	OSO 23.2.0 supports fresh installation and upgrade from 22.3.x. For more information, see *Oracle Communications Operations Services Overlay Installation and Upgrade Guide.*
Oracle Communications Cloud Native Core, cnDBTier	23.2.5	NA	cnDBTier 23.2.5 supports fresh installation and upgrade from 22.4.x, 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, cnDBTier	23.2.4	NA	cnDBTier 23.2.4 supports fresh installation and upgrade from 22.4.x, 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, cnDBTier	23.2.3	NA	cnDBTier 23.2.3 supports fresh installation and upgrade from 22.4.x, 23.1.x, and 23.2.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 2.23.2

Description	NF Version	ATS Version	Upgrade Supported
Oracle Communications Cloud Native Core, cnDBTier	23.2.2	NA	cnDBTier 23.2.2 supports fresh installation and upgrade from 22.4.x, 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, cnDBTier	23.2.1	NA	cnDBTier 23.2.1 supports fresh installation and upgrade from 22.4.x, 23.1.x, and 23.2.0. For more information, see *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, cnDBTier	23.2.0	NA	cnDBTier 23.2.0 supports fresh installation and upgrade from 22.4.x and 23.1.x. For more information, see *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications CD Control Server (CDCS)	23.2.2	NA	CDCS 23.2.2 supports fresh installation and upgrade from 23.1.x and 23.2.x. For more information, see *Oracle Communications CD Control Server Installation and Upgrade Guide.*
Oracle Communications CD Control Server (CDCS)	23.2.1	NA	CDCS 23.2.1 supports fresh installation and upgrade from 23.1.x and 23.2.0. For more information, see *Oracle Communications CD Control Server Installation and Upgrade Guide.*
Oracle Communications CD Control Server (CDCS)	23.2.0	NA	CDCS 23.2.0 supports fresh installation and upgrade from 23.1.x. For more information, see *Oracle Communications CD Control Server Installation and Upgrade Guide.*
Oracle Communications Cloud Native Core, Network Exposure Function (NEF)	23.2.1	23.2.0	NEF 23.2.1 supports fresh installation and upgrade from 22.4.x, 23.1.x, and 23.2.0 to 23.2.1. For more information, see *Oracle Communications Cloud Native Core, Network Exposure Function Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Network Exposure Function (NEF)	23.2.0	23.2.0	NEF 23.2.0 supports fresh installation and upgrade from 22.4.x and 23.1.x. For more information, see *Oracle Communications Cloud Native Core, Network Exposure Function Installation, Upgrade, and Fault Recovery Guide*.

Table 3-1 (Cont.) Media Pack Contents for Oracle Communications Cloud Native Core 2.23.2

Description	NF Version	ATS Version	Upgrade Supported
Oracle Communications Cloud Native Core, Network Repository Function (NRF)	23.2.3	23.2.3	NRF 23.2.3 supports fresh installation and upgrade from 23.1.x and 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 Repository Function (NRF)	23.2.2	23.2.2	NRF 23.2.2 supports fresh installation and upgrade from 23.1.x and 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 Repository Function (NRF)	23.2.1	23.2.1	NRF 23.2.1 supports fresh installation and upgrade from 23.1.x and 23.2.0. 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)	23.2.0	23.2.0	NRF 23.2.0 supports fresh installation and upgrade from 23.1.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)	23.2.0	23.2.0	NSSF 23.2.0 supports fresh installation and upgrade from 23.1.x. The in-service upgrade of NSSF from version 23.1.x to 23.2.0 may experience drop in the success rate. To avoid this and ensure a minimum traffic loss during the upgrade, a workaround is available where pods are upgraded one by one by adding a few parameters in the existing deployments of Ingress Gateway and NsSelection. For more information, see *Oracle Communications Cloud Native Core, Network Slice Selection Function Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Converged Policy (Policy)	23.2.8	23.2.6	Policy 23.2.8 supports fresh installation and upgrade from 22.4.x, 23.1.x, and 23.2.x. For more information, see *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide.*

Table 3-1 (Cont.) Media Pack Contents for Oracle Communications Cloud Native Core 2.23.2

Description	NF Version	ATS Version	Upgrade Supported
Oracle Communications Cloud Native Core, Converged Policy (Policy)	23.2.7	23.2.6	Policy 23.2.7 supports fresh installation and upgrade from 22.4.x, 23.1.x, and 23.2.x. For more information, see *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide.*
Oracle Communications Cloud Native Core, Converged Policy (Policy)	23.2.6	23.2.6	Policy 23.2.6 supports fresh installation and upgrade from 22.4.x, 23.1.x, and 23.2.x. For more information, see *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide.*
Oracle Communications Cloud Native Core, Converged Policy (Policy)	23.2.5	23.2.4	Policy 23.2.5 supports fresh installation and upgrade from 22.4.x, 23.1.x, and 23.2.x. For more information, see *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide.*
Oracle Communications Cloud Native Core, Converged Policy (Policy)	23.2.4	23.2.4	Policy 23.2.4 supports fresh installation and upgrade from 22.4.x, 23.1.x, and 23.2.x. For more information, see *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide.*
Oracle Communications Cloud Native Core, Converged Policy (Policy)	23.2.2	23.2.2	Policy 23.2.2 supports fresh installation and upgrade from 22.4.x, 23.1.x, and 23.2.x. For more information, see *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide.*
Oracle Communications Cloud Native Core, Converged Policy (Policy)	23.2.1	23.2.1	Policy 23.2.1 supports fresh installation and upgrade from 22.4.x, 23.1.x, and 23.2.0. For more information, see *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide.*
Oracle Communications Cloud Native Core, Converged Policy (Policy)	23.2.0	23.2.0	Policy 23.2.0 supports fresh installation and upgrade from 23.1.x and 22.4.x. For more information, see *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide.*

Table 3-1 (Cont.) Media Pack Contents for Oracle Communications Cloud Native Core 2.23.2

Description	NF Version	ATS Version	Upgrade Supported
Oracle Communications Cloud Native Core, Service Communications Proxy (SCP)	23.2.3	23.2.3	SCP 23.2.3 supports fresh installation and upgrade from 22.4.x, 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*.
Oracle Communications Cloud Native Core, Service Communications Proxy (SCP)	23.2.2	23.2.2	SCP 23.2.2 supports fresh installation and upgrade from 22.4.x, 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*.
Oracle Communications Cloud Native Core, Service Communications Proxy (SCP)	23.2.1	23.2.1	SCP 23.2.1 supports fresh installation and upgrade from 22.4.x, 23.1.x, and 23.2.0. 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)	23.2.0	23.2.0	SCP 23.2.0 supports fresh installation and upgrade from 22.4.x and 23.1.x. For more information, see *Oracle Communications Cloud Native Core, Service Communication Proxy Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Security Edge Protection Proxy (SEPP)	23.2.2	23.2.2	SEPP 23.2.2 supports fresh installation and upgrade from 22.4.2, 22.4.3, 22.4.4, 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, Security Edge Protection Proxy (SEPP)	23.2.1	23.2.0	SEPP 23.2.1 supports fresh installation and upgrade from 22.4.2, 22.4.3, 22.4.4, 23.1.x, and 23.2.0. For more information, see *Oracle Communications Cloud Native Core, Security Edge Protection Proxy Installation, Upgrade, and Fault Recovery Guide*.

Table 3-1 (Cont.) Media Pack Contents for Oracle Communications Cloud Native Core 2.23.2

Description	NF Version	ATS Version	Upgrade Supported
Oracle Communications Cloud Native Core, Security Edge Protection Proxy (SEPP)	23.2.0	23.2.0	SEPP 23.2.0 supports fresh installation and upgrade from 22.4.2, 22.4.3, and 23.1.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)	23.2.2	23.2.2	UDR 23.2.2 supports fresh installation and upgrade from 23.2.x, 23.1.x, and 22.4.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)	23.2.1	23.2.1	UDR 23.2.1 supports fresh installation and upgrade from 23.2.0, 22.3.x, 22.4.x, and 23.1.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)	23.2.0	23.2.1	UDR 23.2.0 supports fresh installation and upgrade from 22.3.x, 22.4.x, and 23.1.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	Kubernetes	CNC Console	OCNADD	3GPP
BSF	23.2.4	• 23.2.x • 23.1.x • 22.4.x	• 23.2.x • 23.1.x • 22.4.x	NA	• 22.3.x • 1.10.x • 1.6.x	• 1.25.x • 1.24.x • 1.23.x	23.2.x	NA	• 3GPP TS 29.521 • 3GPP TS 33.501

Table 3-2 (Cont.) Compatibility Matrix

CNC NF	NF Version	CNE	cnDBTier	CDCS	OSO	Kubernetes	CNC Console	OCNADD	3GPP
BSF	23.2.3	• 23.2.x • 23.1.x • 22.4.x	• 23.2.x • 23.1.x • 22.4.x	NA	• 22.3.x • 1.10.x • 1.6.x	• 1.25.x • 1.24.x • 1.23.x	23.2.x	NA	• 3GPP TS 29.521 • 3GPP TS 33.501
BSF	23.2.2	• 23.2.x • 23.1.x • 22.4.x	• 23.2.x • 23.1.x • 22.4.x	NA	• 22.3.x • 1.10.x • 1.6.x	• 1.25.x • 1.24.x • 1.23.x	23.2.x	NA	• 3GPP TS 29.521 • 3GPP TS 33.501
BSF	23.2.1	• 23.2.x • 23.1.x • 22.4.x	• 23.2.x • 23.1.x • 22.4.x	NA	• 22.3.x • 1.10.x • 1.6.x	• 1.25.x • 1.24.x • 1.23.x	23.2.x	NA	• 3GPP TS 29.521 • 3GPP TS 33.501
BSF	23.2.0	• 23.2.0 • 23.1.x • 22.4.x	• 23.2.0 • 23.1.x • 22.4.x	NA	• 22.3.x • 1.10.x • 1.6.x	• 1.25.x • 1.24.x • 1.23.x	23.2.0	NA	• 3GPP TS 29.521 • 3GPP TS 33.501
CDCS	23.2.2	• 23.2.x • 23.1.x • 22.4.x	NA	NA	NA	1.25.x	NA	NA	NA
CDCS	23.2.1	• 23.2.x • 23.1.x • 22.4.x	NA	NA	NA	1.25.x	NA	NA	NA
CDCS	23.2.0	• 23.2.x • 23.1.x • 22.4.x	NA	NA	NA	1.25.x	NA	NA	NA
CNC Console	23.2.2	• 23.2.x • 23.1.x • 22.4.x	• 23.2.x • 23.1.x • 22.4.x	• 23.2.x • 23.1.x • 22.4.x	• 23.2.x • 22.3.x • 1.10.x	• 1.25.x • 1.24.x • 1.23.x	NA	23.2.x	NA
CNC Console	23.2.1	• 23.2.x • 23.1.x • 22.4.x	• 23.2.x • 23.1.x • 22.4.x	• 23.2.x • 23.1.x • 22.4.x	• 23.2.x • 22.3.x • 1.10.x	• 1.25.x • 1.24.x • 1.23.x	NA	23.2.x	NA

Table 3-2 (Cont.) Compatibility Matrix

CNC NF	NF Version	CNE	cnDBTier	CDCS	OSO	Kubernetes	CNC Console	OCNADD	3GPP
CNC Console	23.2.0	• 23.2.x • 23.1.x • 22.4.x	• 23.2.x • 23.1.x • 22.4.x	• 23.2.x • 23.1.x • 22.4.x	• 23.2.x • 22.3.x • 1.10.x	• 1.25.x • 1.24.x • 1.23.x	NA	23.2.0	NA
CNE	23.2.6	NA	NA	NA	NA	1.25.x	NA	NA	NA
CNE	23.2.5	NA	NA	NA	NA	1.25.x	NA	NA	NA
CNE	23.2.4	NA	NA	NA	NA	1.25.x	NA	NA	NA
CNE	23.2.3	NA	NA	NA	NA	1.25.x	NA	NA	NA
CNE	23.2.1	NA	NA	NA	NA	1.25.x	NA	NA	NA
CNE	23.2.0	NA	NA	NA	NA	1.25.x	NA	NA	NA
cnDBTier	23.2.5	• 23.2.x • 23.1.x • 22.4.x	NA	NA	NA	• 1.25.x • 1.24.x • 1.23.x	NA	NA	NA
cnDBTier	23.2.4	• 23.2.x • 23.1.x • 22.4.x	NA	NA	NA	• 1.25.x • 1.24.x • 1.23.x	NA	NA	NA
cnDBTier	23.2.3	• 23.2.x • 23.1.x • 22.4.x	NA	NA	NA	• 1.25.x • 1.24.x • 1.23.x	NA	NA	NA
cnDBTier	23.2.2	• 23.2.x • 23.1.x • 22.4.x	NA	NA	NA	• 1.25.x • 1.24.x • 1.23.x	NA	NA	NA
cnDBTier	23.2.1	• 23.2.x • 23.1.x • 22.4.x	NA	NA	NA	• 1.25.x • 1.24.x • 1.23.x	NA	NA	NA
cnDBTier	23.2.0	• 23.2.x • 23.1.x • 22.4.x	NA	NA	NA	• 1.25.x • 1.24.x • 1.23.x	NA	NA	NA

Table 3-2 (Cont.) Compatibility Matrix

CNC NF	NF Version	CNE	cnDBTier	CDCS	OSO	Kubernetes	CNC Console	OCNADD	3GPP
NEF	23.2.1	• 23.2.x • 23.1.x • 22.4.x	• 23.2.x • 23.1.x • 22.4.x	NA	NA	• 1.25.x • 1.24.x • 1.23.x	NA	NA	• 3GPP TS 29.122 v16.10.0 • 3GPP TS 23.222 v16.9.0 • 3GPP TS 23.501 v 16.10.0 • 3GPP TS 23.502 v 16.10.0 • 3GPP TS 29.514 v16.10.0 • 3GPP TS 29.521 v16.10 • 3GPP TS 29.503 v16.14.0 • 3GPP TS 29.515 v16.7 • 3GPP TS 29.222 v16.5.0 • 3GPP TS 29.500 v16.6.0 • 3GPP TS29.501 v16.6.0 • 3GPP TS 29.522 v16.10 • 3GPP TS29.510 v16.6.0 • 3GPP TS

Table 3-2 (Cont.) Compatibility Matrix

CNC NF	NF Version	CNE	cnDBTier	CDCS	OSO	Kubernetes	CNC Console	OCNADD	3GPP
									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

Table 3-2 (Cont.) Compatibility Matrix

CNC NF	NF Version	CNE	cnDBTier	CDCS	OSO	Kubernetes	CNC Console	OCNADD	3GPP
NEF	23.2.0	• 23.2.x • 23.1.x • 22.4.x	• 23.2.x • 23.1.x • 22.4.x	NA	NA	• 1.25.x • 1.24.x • 1.23.x	NA	NA	• 3GPP TS 29.122 v16.10.0 • 3GPP TS 23.222 v16.9.0 • 3GPP TS 23.501 v 16.10.0 • 3GPP TS 23.502 v 16.10.0 • 3GPP TS 29.514 v16.10.0 • 3GPP TS 29.521 v16.10 • 3GPP TS 29.503 v16.14.0 • 3GPP TS 29.515 v16.7 • 3GPP TS 29.222 v16.5.0 • 3GPP TS 29.500 v16.6.0 • 3GPP TS29.501 v16.6.0 • 3GPP TS 29.522 v16.10 • 3GPP TS29.510 v16.6.0 • 3GPP TS

Table 3-2 (Cont.) Compatibility Matrix

CNC NF	NF Version	CNE	cnDBTier	CDCS	OSO	Kubernetes	CNC Console	OCNADD	3GPP
									• 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
NRF	23.2.3	• 23.2.x • 23.1.x • 22.4.x	• 23.2.x • 23.1.x • 22.4.x	NA	• 22.3.x • 1.10.x	• 1.25.x • 1.24.x • 1.23.x	23.2.x	23.2.0	• 3GPP TS 29.510 v15.5 • 3GPP TS 29.510 v16.3.0 • 3GPP TS 29.510 v16.7
NRF	23.2.2	• 23.2.x • 23.1.x • 22.4.x	• 23.2.x • 23.1.x • 22.4.x	NA	• 22.3.x • 1.10.x	• 1.25.x • 1.24.x • 1.23.x	23.2.x	23.2.0	• 3GPP TS 29.510 v15.5 • 3GPP TS 29.510 v16.3.0 • 3GPP TS 29.510 v16.7

Table 3-2 (Cont.) Compatibility Matrix

CNC NF	NF Version	CNE	cnDBTier	CDCS	OSO	Kubernetes	CNC Console	OCNADD	3GPP
NRF	23.2.1	• 23.2.x • 23.1.x • 22.4.x	• 23.2.x • 23.1.x • 22.4.x	NA	• 22.3.x • 1.10.x	• 1.25.x • 1.24.x • 1.23.x	23.2.x	23.2.0	• 3GPP TS 29.510 v15.5 • 3GPP TS 29.510 v16.3.0 • 3GPP TS 29.510 v16.7
NRF	23.2.0	• 23.2.x • 23.1.x • 22.4.x	• 23.2.x • 23.1.x • 22.4.x	NA	• 22.3.x • 1.10.x	• 1.25.x • 1.24.x • 1.23.x	23.2.x	23.2.0	• 3GPP TS 29.510 v15.5 • 3GPP TS 29.510 v16.3.0 • 3GPP TS 29.510 v16.7
NSSF	23.2.0	• 23.2.x • 23.1.x • 22.4.x	• 23.2.x • 23.1.x • 22.4.x	NA	• 22.3.x • 1.10.x	• 1.25.x • 1.24.x • 1.23.x	23.2.x	NA	• 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

Table 3-2 (Cont.) Compatibility Matrix

CNC NF	NF Version	CNE	cnDBTier	CDCS	OSO	Kubernetes	CNC Console	OCNADD	3GPP
Policy	23.2.8	• 23.2.x • 23.1.x • 22.4.x	• 23.2.x • 23.1.x • 22.4.x	NA	• 22.3.x • 1.10.x	• 1.25.x • 1.24.x • 1.23.x	23.2.x	NA	• 3GPP TS 33.501 v17.7.0 • 3GPP TS 23.503v 15.7.0 • 3GPP TS 29.500v 16.3.0 • 3GPP TS 23.203v 15.4.0 • 3GPP TS 29.507v 15.5.0 • 3GPP TS 29.512v 16.4 • 3GPP TS 29.513v 15.5.0 • 3GPP TS 29.514v 16.4.0 • 3GPP TS 29.519v 15.5.0 • 3GPP TS 29.521v 16.5.0 • 3GPP TS 29.525v 15.3.0 • 3GPP TS 29.594v 15.5.0 • 3GPP TS 29.214v 15.4.0 • 3GPP TS

Table 3-2 (Cont.) Compatibility Matrix

CNC NF	NF Version	CNE	cnDBTier	CDCS	OSO	Kubernetes	CNC Console	OCNADD	3GPP
									29.212v 15.4 • 3GPP TS 29.213v 15.4 • 3GPP TS 29.215v 15.1.0 • 3GPP TS 29.219v 15.1.0 • 3GPP TS 29.329v 14.0.0 • 3GPP TS 29.335v 13.1.0

Table 3-2 (Cont.) Compatibility Matrix

CNC NF	NF Version	CNE	cnDBTier	CDCS	OSO	Kubernetes	CNC Console	OCNADD	3GPP
Policy	23.2.7	• 23.2.x • 23.1.x • 22.4.x	• 23.2.x • 23.1.x • 22.4.x	NA	• 22.3.x • 1.10.x	• 1.25.x • 1.24.x • 1.23.x	23.2.x	NA	• 3GPP TS 33.501 v17.7.0 • 3GPP TS 23.503v 15.7.0 • 3GPP TS 29.500v 16.3.0 • 3GPP TS 23.203v 15.4.0 • 3GPP TS 29.507v 15.5.0 • 3GPP TS 29.512v 16.4 • 3GPP TS 29.513v 15.5.0 • 3GPP TS 29.514v 16.4.0 • 3GPP TS 29.519v 15.5.0 • 3GPP TS 29.521v 16.5.0 • 3GPP TS 29.525v 15.3.0 • 3GPP TS 29.594v 15.5.0 • 3GPP TS 29.214v 15.4.0 • 3GPP TS

Table 3-2 (Cont.) Compatibility Matrix

CNC NF	NF Version	CNE	cnDBTier	CDCS	OSO	Kubernetes	CNC Console	OCNADD	3GPP
									29.212v 15.4 • 3GPP TS 29.213v 15.4 • 3GPP TS 29.215v 15.1.0 • 3GPP TS 29.219v 15.1.0 • 3GPP TS 29.329v 14.0.0 • 3GPP TS 29.335v 13.1.0

Table 3-2 (Cont.) Compatibility Matrix

CNC NF	NF Version	CNE	cnDBTier	CDCS	OSO	Kubernetes	CNC Console	OCNADD	3GPP
Policy	23.2.6	• 23.2.x • 23.1.x • 22.4.x	• 23.2.x • 23.1.x • 22.4.x	NA	• 22.3.x • 1.10.x	• 1.25.x • 1.24.x • 1.23.x	23.2.x	NA	• 3GPP TS 33.501 v17.7.0 • 3GPP TS 23.503v 15.7.0 • 3GPP TS 29.500v 16.3.0 • 3GPP TS 23.203v 15.4.0 • 3GPP TS 29.507v 15.5.0 • 3GPP TS 29.512v 16.4 • 3GPP TS 29.513v 15.5.0 • 3GPP TS 29.514v 16.4.0 • 3GPP TS 29.519v 15.5.0 • 3GPP TS 29.521v 16.5.0 • 3GPP TS 29.525v 15.3.0 • 3GPP TS 29.594v 15.5.0 • 3GPP TS 29.214v 15.4.0 • 3GPP TS

Table 3-2 (Cont.) Compatibility Matrix

CNC NF	NF Version	CNE	cnDBTier	CDCS	OSO	Kubernetes	CNC Console	OCNADD	3GPP
									29.212v 15.4 • 3GPP TS 29.213v 15.4 • 3GPP TS 29.215v 15.1.0 • 3GPP TS 29.219v 15.1.0 • 3GPP TS 29.329v 14.0.0 • 3GPP TS 29.335v 13.1.0

Table 3-2 (Cont.) Compatibility Matrix

CNC NF	NF Version	CNE	cnDBTier	CDCS	OSO	Kubernetes	CNC Console	OCNADD	3GPP
Policy	23.2.5	• 23.2.x • 23.1.x • 22.4.x	• 23.2.x • 23.1.x • 22.4.x	NA	• 22.3.x • 1.10.x	• 1.25.x • 1.24.x • 1.23.x	23.2.x	NA	• 3GPP TS 23.501 v17.7.0 • 3GPP TS 23.503v 15.7.0 • 3GPP TS 29.500v 16.3.0 • 3GPP TS 23.203v 15.4.0 • 3GPP TS 29.507v 15.5.0 • 3GPP TS 29.512v 16.4 • 3GPP TS 29.513v 15.5.0 • 3GPP TS 29.514v 16.4.0 • 3GPP TS 29.519v 15.5.0 • 3GPP TS 29.521v 16.5.0 • 3GPP TS 29.525v 15.3.0 • 3GPP TS 29.594v 15.5.0 • 3GPP TS 29.214v 15.4.0 • 3GPP TS

Table 3-2 (Cont.) Compatibility Matrix

CNC NF	NF Version	CNE	cnDBTier	CDCS	OSO	Kubernetes	CNC Console	OCNADD	3GPP
									• 29.212v 15.4 • 3GPP TS 29.213v 15.4 • 3GPP TS 29.215v 15.1.0 • 3GPP TS 29.219v 15.1.0 • 3GPP TS 29.329v 14.0.0 • 3GPP TS 29.335v 13.1.0

Table 3-2 (Cont.) Compatibility Matrix

CNC NF	NF Version	CNE	cnDBTier	CDCS	OSO	Kubernetes	CNC Console	OCNADD	3GPP
Policy	23.2.4	• 23.2.x • 23.1.x • 22.4.x	• 23.2.x • 23.1.x • 22.4.x	NA	• 22.3.x • 1.10.x	• 1.25.x • 1.24.x • 1.23.x	23.2.x	NA	• 3GPP TS 23.501 v17.7.0 • 3GPP TS 23.503v 15.7.0 • 3GPP TS 29.500v 16.3.0 • 3GPP TS 23.203v 15.4.0 • 3GPP TS 29.507v 15.5.0 • 3GPP TS 29.512v 16.4 • 3GPP TS 29.513v 15.5.0 • 3GPP TS 29.514v 16.4.0 • 3GPP TS 29.519v 15.5.0 • 3GPP TS 29.521v 16.5.0 • 3GPP TS 29.525v 15.3.0 • 3GPP TS 29.594v 15.5.0 • 3GPP TS 29.214v 15.4.0 • 3GPP TS

Table 3-2 (Cont.) Compatibility Matrix

CNC NF	NF Version	CNE	cnDBTier	CDCS	OSO	Kubernetes	CNC Console	OCNADD	3GPP
									29.212v 15.4 • 3GPP TS 29.213v 15.4 • 3GPP TS 29.215v 15.1.0 • 3GPP TS 29.219v 15.1.0 • 3GPP TS 29.329v 14.0.0 • 3GPP TS 29.335v 13.1.0

Table 3-2 (Cont.) Compatibility Matrix

CNC NF	NF Version	CNE	cnDBTier	CDCS	OSO	Kubernetes	CNC Console	OCNADD	3GPP
Policy	23.2.2	• 23.2.x • 23.1.x • 22.4.x	• 23.2.x • 23.1.x • 22.4.x	NA	• 22.3.x • 1.10.x	• 1.25.x • 1.24.x • 1.23.x	23.2.x	NA	• 3GPP TS 23.501 • 3GPP TS 23.502 • 3GPP TS 23.503 • 3GPP TS 29.500 • 3GPP TS 29.504 • 3GPP TS 29.510 • 3GPP TS 29.507 • 3GPP TS 29.512 • 3GPP TS 29.513 • 3GPP TS 29.514 • 3GPP TS 29.519 • 3GPP TS 29.521 • 3GPP TS 29.525 • 3GPP TS 29.594 • 3GPP TS 29.214 • 3GPP TS 29.212

Table 3-2 (Cont.) Compatibility Matrix

CNC NF	NF Version	CNE	cnDBTier	CDCS	OSO	Kubernetes	CNC Console	OCNADD	3GPP
Policy	23.2.1	• 23.2.x • 23.1.x • 22.4.x	• 23.2.x • 23.1.x • 22.4.x	NA	• 22.3.x • 1.10.x	• 1.25.x • 1.24.x • 1.23.x	23.2.x	NA	• 3GPP TS 23.501 • 3GPP TS 23.502 • 3GPP TS 23.503 • 3GPP TS 29.500 • 3GPP TS 29.504 • 3GPP TS 29.510 • 3GPP TS 29.507 • 3GPP TS 29.512 • 3GPP TS 29.513 • 3GPP TS 29.514 • 3GPP TS 29.519 • 3GPP TS 29.521 • 3GPP TS 29.525 • 3GPP TS 29.594 • 3GPP TS 29.214 • 3GPP TS 29.212

Table 3-2 (Cont.) Compatibility Matrix

CNC NF	NF Version	CNE	cnDBTier	CDCS	OSO	Kubernetes	CNC Console	OCNADD	3GPP
Policy	23.2.0	• 23.2.x • 23.1.x • 22.4.x	• 23.2.x • 23.1.x • 22.4.x	NA	• 22.3.x • 1.10.x	• 1.25.x • 1.24.x • 1.23.x	23.2.0	NA	• 3GPP TS 23.501 • 3GPP TS 23.502 • 3GPP TS 23.503 • 3GPP TS 29.500 • 3GPP TS 29.504 • 3GPP TS 29.510 • 3GPP TS 29.507 • 3GPP TS 29.512 • 3GPP TS 29.513 • 3GPP TS 29.514 • 3GPP TS 29.519 • 3GPP TS 29.521 • 3GPP TS 29.525 • 3GPP TS 29.594 • 3GPP TS 29.214 • 3GPP TS 29.212

Table 3-2 (Cont.) Compatibility Matrix

CNC NF	NF Version	CNE	cnDBTier	CDCS	OSO	Kubernetes	CNC Console	OCNADD	3GPP
SCP	23.2.3	• 23.2.x • 23.1.x • 22.4.x	• 23.2.x • 23.1.x • 22.4.x	• 23.2.x • 23.1.x • 22.4.x	• 23.2.x • 22.3.x • 1.10.x	• 1.25.x • 1.24.x • 1.23.x	23.2.x	23.2.0	• 3GPP TS 29.510 v16.10.0
SCP	23.2.2	• 23.2.x • 23.1.x • 22.4.x	• 23.2.x • 23.1.x • 22.4.x	• 23.2.x • 23.1.x • 22.4.x	• 23.2.x • 22.3.x • 1.10.x	• 1.25.x • 1.24.x • 1.23.x	23.2.x	23.2.0	• 3GPP TS 29.510 v16.10.0
SCP	23.2.1	• 23.2.x • 23.1.x • 22.4.x	• 23.2.x • 23.1.x • 22.4.x	• 23.2.x • 23.1.x • 22.4.x	• 23.2.x • 22.3.x • 1.10.x	• 1.25.x • 1.24.x • 1.23.x	23.2.x	23.2.0	• 3GPP TS 29.510 v16.10.0
SCP	23.2.0	• 23.2.x • 23.1.x • 22.4.x	• 23.2.x • 23.1.x • 22.4.x	• 23.2.x • 23.1.x • 22.4.x	• 23.2.x • 22.3.x • 1.10.x	• 1.25.x • 1.24.x • 1.23.x	23.2.x	23.2.0	• 3GPP TS 29.510 v16.10.0
SEPP	23.2.2	• 23.2.x • 23.1.x • 22.4.x	• 23.2.x • 23.1.x • 22.4.x	• 23.2.x • 23.1.x • 22.4.x	22.3.x	• 1.25.x • 1.24.x • 1.23.x	23.2.x	23.2.0	• 3GPP TS 23.501 v16.7.0 • 3GPP TS 23.502 v16.7.0 • 3GPP TS 29.500 v16.6.0 • 3GPP TS 29.501 v16.5.0 • 3GPP TS 29.510 v16.6.0 • 3GPP TS 29.573 v16.3.0

Table 3-2 (Cont.) Compatibility Matrix

CNC NF	NF Version	CNE	cnDBTier	CDCS	OSO	Kubernetes	CNC Console	OCNADD	3GPP
SEPP	23.2.1	• 23.2.x • 23.1.x • 22.4.x	• 23.2.x • 23.1.x • 22.4.x	• 23.2.x • 23.1.x • 22.4.x	22.3.x	• 1.25.x • 1.24.x • 1.23.x	23.2.x	23.2.0	• 3GPP TS 23.501 v17.6.0 • 3GPP TS 23.502 v17.6.0 • 3GPP TS 29.500 v17.8.0 • 3GPP TS 29.501 v17.7.0 • 3GPP TS 29.510 v17.7.0 • 3GPP TS 33.501 v17.7.0 • 3GPP TS 33.117 v17.1.0 • 3GPP TS 33.210 v17.1.0

Table 3-2 (Cont.) Compatibility Matrix

CNC NF	NF Version	CNE	cnDBTier	CDCS	OSO	Kubernetes	CNC Console	OCNADD	3GPP
SEPP	23.2.0	• 23.2.x • 23.1.x • 22.4.x	• 23.2.x • 23.1.x • 22.4.x	• 23.2.x • 23.1.x • 22.4.x	22.3.x	• 1.25.x • 1.24.x • 1.23.x	23.2.x	23.2.0	• 3GPP TS 23.501 v17.6.0 • 3GPP TS 23.502 v17.6.0 • 3GPP TS 29.500 v17.8.0 • 3GPP TS 29.501 v17.7.0 • 3GPP TS 29.510 v17.7.0 • 3GPP TS 33.501 v17.7.0 • 3GPP TS 33.117 v17.1.0 • 3GPP TS 33.210 v17.1.0
UDR	23.2.2	• 23.2.x • 23.1.x • 22.4.x	• 23.2.x • 23.1.x • 22.4.x	NA	• 23.2.x • 22.3.x • 1.6.x	• 1.25.x • 1.24.x • 1.23.x	23.2.x	NA	• 3GPP TS 29.505 v15.4.0 • 3GPP TS 29.504 v16.2.0 • 3GPP TS 29.519 v16.2.0 • 3GPP TS 29.511 v17.2.0

Table 3-2 (Cont.) Compatibility Matrix

CNC NF	NF Version	CNE	cnDBTier	CDCS	OSO	Kubernetes	CNC Console	OCNADD	3GPP
UDR	23.2.1	• 23.2.x • 23.1.x • 22.4.x	• 23.2.x • 23.1.x • 22.4.x	NA	• 23.2.x • 22.3.x • 1.6.x	• 1.25.x • 1.24.x • 1.23.x	23.2.x	NA	• 3GPP TS 29.505 v15.4.0 • 3GPP TS 29.504 v16.2.0 • 3GPP TS 29.519 v16.2.0 • 3GPP TS 29.511 v17.2.0
UDR	23.2.0	• 23.2.x • 23.1.x • 22.4.x	• 23.2.x • 23.1.x • 22.4.x	NA	• 23.2.x • 22.3.x • 1.6.x	• 1.25.x • 1.24.x • 1.23.x	23.2.x	NA	• 3GPP TS 29.505 v15.4.0 • 3GPP TS 29.504 v16.2.0 • 3GPP TS 29.519 v16.2.0 • 3GPP TS 29.511 v17.2.0

3.3 Common Microservices Load Lineup

This section provides information about common microservices and ATS for the specific NF versions in Oracle Communications Cloud Native Core Release 2.23.2.

Table 3-3 Common Microservices Load Lineup for Network Functions

CNC NF	NF Version	Alternate Route Svc	App-Info	ASM Configuration	ATS Framework	Config-Server	Debug-tool	Egress Gateway	Ingress Gateway	Helm Test	Mediation	NRF-Client	Perf-Info
BSF	23.2.4	23.2.12	23.2.7	23.2.4	23.2.2	23.2.7	23.2.1	23.2.12	23.2.12	23.2.1	NA	23.2.2	23.2.7
BSF	23.2.3	23.2.12	23.2.6	23.2.3	23.2.2	23.2.6	23.2.1	23.2.12	23.2.12	23.2.1	NA	23.2.2	23.2.6
BSF	23.2.2	23.2.9	23.2.4	23.2.2	23.2.2	23.2.4	23.2.0	23.2.9	23.2.9	23.2.0	NA	23.2.1	23.2.4

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

CNC NF	NF Version	Alternate Route Svc	App-Info	ASM Configuration	ATS Framework	Config-Server	Debug-tool	Egress Gateway	Ingress Gateway	Helm Test	Mediation	NRF-Client	Perf-Info
BSF	23.2.1	23.2.7	23.2.1	23.2.0	23.2.1	23.2.1	23.2.0	23.2.7	23.2.7	23.2.0	NA	23.2.1	23.2.1
BSF	23.2.0	23.2.6	23.2.0	23.2.0	23.2.1	23.2.0	23.2.0	23.2.6	23.2.6	23.2.0	NA	23.2.1	23.2.0
CNC Console	23.2.2	NA	NA	NA	NA	NA	23.2.1	NA	23.2.10	23.2.0	NA	NA	NA
CNC Console	23.2.1	NA	NA	NA	NA	NA	23.2.0	NA	23.2.4	23.2.0	NA	NA	NA
CNC Console	23.2.0	NA	NA	NA	NA	NA	23.2.0	NA	23.2.4	23.2.0	NA	NA	NA
NEF	23.2.1	NA	23.2.0	NA	23.2.1	23.2.0	23.2.0	23.2.4	23.2.4	23.2.0	NA	23.2.0	23.2.0
NEF	23.2.0	NA	23.2.0	NA	23.2.1	23.2.0	23.2.0	23.2.4	23.2.4	23.2.0	NA	23.2.0	23.2.0
NRF	23.2.3	23.2.13	23.2.4	23.2.1	23.2.2	NA	23.2.1	23.2.13	23.2.13	23.2.0	NA	NA	23.2.4
NRF	23.2.2	23.2.10	23.2.4	23.2.1	23.2.2	NA	23.2.1	23.2.10	23.2.10	23.2.0	NA	NA	23.2.4
NRF	23.2.1	23.2.8	23.2.1	23.2.1	23.2.1	NA	23.2.0	23.2.8	23.2.8	23.2.0	NA	NA	23.2.0
NRF	23.2.0	23.2.4	23.2.0	23.2.0	23.2.1	NA	23.2.0	23.2.4	23.2.4	23.2.0	NA	NA	23.2.0
NSSF	23.2.0	23.2.4	23.2.0	23.2.0	23.2.1	23.2.3	23.2.0	23.2.4	23.2.4	23.2.0	NA	23.2.0	23.2.0
Policy	23.2.8	23.2.12	23.2.8	23.2.8	23.2.2	23.2.8	23.2.1	23.2.12	23.2.12	23.2.0	NA	23.2.2	23.2.8
Policy	23.2.7	23.2.12	23.2.7	23.2.7	23.2.2	23.2.7	23.2.1	23.2.12	23.2.12	23.2.0	NA	23.2.2	23.2.7
Policy	23.2.6	23.2.12	23.2.6	23.2.6	23.2.2	23.2.6	23.2.1	23.2.12	23.2.12	23.2.0	NA	23.2.2	23.2.6
Policy	23.2.5	23.2.9	23.2.5	23.2.5	23.2.1	23.2.5	23.2.0	23.2.9	23.2.9	23.2.0	NA	23.2.1	23.2.5
Policy	23.2.4	23.2.9	23.2.4	23.2.4	23.2.1	23.2.4	23.2.0	23.2.9	23.2.9	23.2.0	NA	23.2.1	23.2.4
Policy	23.2.2	23.2.7	23.2.2	23.2.2	23.2.1	23.2.7	23.2.0	23.2.7	23.2.7	23.2.0	NA	23.2.1	23.2.2
Policy	23.2.1	23.2.7	23.2.1	23.2.0	23.2.1	23.2.1	23.2.0	23.2.7	23.2.7	23.2.0	NA	23.2.1	23.2.1
Policy	23.2.0	23.2.6	23.2.0	23.2.0	23.2.1	23.2.0	23.2.0	23.2.6	23.2.6	23.2.0	NA	23.2.1	23.2.0
SCP	23.2.3	NA	NA	23.2.1	23.2.1	NA	23.2.0	NA	NA	23.2.0	23.2.1	NA	NA
SCP	23.2.2	NA	NA	23.2.1	23.2.1	NA	23.2.0	NA	NA	23.2.0	23.2.0	NA	NA
SCP	23.2.1	NA	NA	23.2.1	23.2.1	NA	23.2.0	NA	NA	23.2.0	23.2.0	NA	NA
SCP	23.2.0	NA	NA	23.2.0	23.2.1	NA	23.2.0	NA	NA	23.2.0	23.2.0	NA	NA
SEPP	23.2.2	NA	23.2.4	23.2.0	23.2.2	23.2.4	23.2.1	23.2.10	23.2.10	23.2.0	23.2.1	23.2.2	23.2.4
SEPP	23.2.1	NA	23.2.0	23.2.0	23.2.0	23.2.0	23.2.0	23.2.7	23.2.7	23.2.0	23.2.0	23.2.0	23.2.0
SEPP	23.2.0	NA	23.2.0	23.2.0	23.2.0	23.2.0	23.2.0	23.2.3	23.2.3	23.2.0	23.2.0	23.2.0	23.2.0
UDR	23.2.2	23.2.13	23.2.4	23.2.0	23.2.1	23.2.4	23.2.0	23.2.13	23.2.13	23.2.0	NA	23.2.0	23.2.4
UDR	23.2.1	23.2.13	23.2.0	23.2.0	23.2.1	23.2.0	23.2.0	23.2.13	23.2.13	23.2.0	NA	23.2.0	23.2.0
UDR	23.2.0	23.2.4	23.2.0	23.2.0	23.2.1	23.2.0	23.2.0	23.2.4	23.2.4	23.2.0	NA	23.2.0	23.2.0

3.4 Security Certification Declaration

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

Table 3-4 Security Certification Declaration

CNC NF	NF Version	Systems test on functional and security features	Regression testing on security configuration	Vulnerability testing	Fuzz testing on external interfaces
BSF	23.2.4	Oct 3, 2023	Oct 10, 2023	Oct 10, 2023	Oct 2, 2023
BSF	23.2.3	Oct 3, 2023	Oct 10, 2023	Oct 10, 2023	Oct 2, 2023
BSF	23.2.2	July 18, 2023	July 18, 2023	July 25, 2023	July 3, 2023
BSF	23.2.1	July 18, 2023	July 18, 2023	July 25, 2023	July 3, 2023
BSF	23.2.0	May 30, 2023	May 24, 2023	May 31, 2023	May 23, 2023
CNC Console	23.2.2	Oct 9, 2023	Oct 9, 2023	Oct 9, 2023	May 11, 2023
CNC Console	23.2.1	May 19, 2023	May 19, 2023	May 11, 2023	May 11, 2023
CNC Console	23.2.0	May 19, 2023	May 19, 2023	May 11, 2023	May 11, 2023
NEF	23.2.1	Oct 16, 2023	May 3, 2023	May 3, 2023	May 3, 2023
NEF	23.2.0	May 3, 2023	May 3, 2023	May 3, 2023	May 3, 2023
NRF	23.2.3	Oct 12, 2023	Oct 12, 2023	Oct 12, 2023	Oct 12, 2023
NRF	23.2.2	Oct 12, 2023	Oct 12, 2023	Oct 12, 2023	Oct 12, 2023
NRF	23.2.1	Sep 15, 2023	Sep 15, 2023	Sep 15, 2023	Sep 15, 2023
NRF	23.2.0	May 23, 2023	May 23, 2023	May 23, 2023	May 23, 2023
NSSF	23.2.0	May 9, 2023	May 9, 2023	May 9, 2023	May 9, 2023
Policy	23.2.8	March 7, 2024	Jan 8, 2024	Jan 8, 2024	Oct 10, 2023
Policy	23.2.7	Nov 13, 2023	Nov 13, 2023	Nov 17, 2023	Oct 10, 2023
Policy	23.2.6	Nov 13, 2023	Nov 13, 2023	Nov 17, 2023	Oct 10, 2023
Policy	23.2.5	Oct 16, 2023	Oct 2, 2023	Oct 16, 2023	Oct 3, 2023
Policy	23.2.4	July 18, 2023	July 18, 2023	July 25, 2023	July 12, 2023
Policy	23.2.2	July 18, 2023	July 18, 2023	July 25, 2023	July 12, 2023
Policy	23.2.1	July 18, 2023	July 18, 2023	July 25, 2023	July 3, 2023
Policy	23.2.0	May 26, 2023	May 31, 2023	May 31, 2023	May 17, 2023
SCP	23.2.3	Oct 13, 2023	Oct 13, 2023	Oct 13, 2023	Oct 13, 2023
SCP	23.2.2	May 24, 2023	May 24, 2023	May 24, 2023	May 24, 2023
SCP	23.2.1	May 24, 2023	May 24, 2023	May 24, 2023	May 24, 2023
SCP	23.2.0	May 24, 2023	May 24, 2023	May 24, 2023	May 24, 2023
SEPP	23.2.2	Oct 13, 2023	Oct 13, 2023	Oct 13, 2023	Oct 13, 2023
SEPP	23.2.1	August 22, 2023	August 22, 2023	August 22, 2023	NA
SEPP	23.2.0	May 26, 2023	May 26, 2023	May 26, 2023	May 26, 2023
UDR	23.2.2	NA	May 16, 2023	May 16, 2023	May 16, 2023
UDR	23.2.1	NA	May 16, 2023	May 16, 2023	May 16, 2023
UDR	23.2.0	NA	May 16, 2023	May 16, 2023	May 16, 2023

3.5 Documentation Pack

All documents for Oracle Communications Cloud Native Core (CNC) 2.23.2 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 2.23.2.

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 2.23.2.

4.2.1 BSF Resolved Bugs

Table 4-1 BSF 23.2.4 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
36124195	CHF connector HTTP2 Remote Reset causing N28 create failure	CHF connector was failing with concurrent modification exception during validation of SBI binding header value while sending request messages with 3GPP SBI binding header.	2	23.2.3

> **Note:**
>
> Resolved bugs from 23.2.x have been forward ported to Release 23.2.4.

BSF 23.2.3 Resolved Bugs

There are no new resolved bugs in this release. Resolved bugs from 23.2.x have been forward ported to Release 23.2.3.

Table 4-2 BSF 23.2.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
35791822	BSF Pcfbindings not found session	BSF Management Service returned "404 NOT_FOUND" instead of "204 NO_CONTENT" when no pcfBinding was found with the queryParameters of the GET request.	2	23.1.0

Table 4-3 BSF 23.2.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
35516391	single site 35K TPS param "envXnioTaskThreadPoolSize" is set to 50	BSF was not able to handle 35K TPS traffic smoothly when the parameter *envXnioTaskThreadPoolSize* was set to 50.	3	23.2.0
35676108	diam-gw logging enhancement for IP-CAN_SESSION_NOT_AVAILABLE (5065)	When PCF Diameter Gateway was configured with logging level WARN, it did not print any logs while responding with DIAMETER error. For example, IP-CAN_SESSION_NOT_AVAILABLE (3GPP,5065).	3	23.2.0

BSF ATS 23.2.1 Resolved Bugs

There are no new BSF ATS bugs in this release. Resolved bugs from 22.4.x have been forward ported to Release 23.2.1.

Table 4-4 BSF 23.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
35033402	NRF retry fails in ATS System	ATS feature, NRF_SessionRetry_virtualNRFresolution, failed during regression run, due to race condition in common_config server version number logic.	2	22.4.0
35329797	AppInfo Service deployment do not read 'port' parameter from custom yaml file	During appinfo deployment, PERFINFO_PORT parameter value was read, instead of the customizable parameter `perfInfoHttp` value set by the customer.	2	22.4.2

Note:

Resolved bugs from 22.4.x and 23.1.x have been forward ported to Release 23.2.0.

Table 4-5 BSF ATS 23.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
35425572	NRF retry fails in ATS System	ATS feature, `NRF_SessionRetry_virtualNRFresolution`, failed during regression run, due to race condition in common_config server version number logic.	2	22.4.0

> **Note:**
>
> Resolved bugs from 23.1.x have been forward ported to Release 23.2.0.

4.2.2 CDCS Resolved Bugs

CDCS 23.2.2 Resolved Bugs

There are no resolved bugs in this release.

Table 4-6 CDCS 23.2.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35580056	Pipelines not waiting for helm commands to complete.	Certain pipelines in CDCS are not completed successfully and their status is reported as successful even when the command fails. Hence, the `--wait` flag has been added to all the Helm commands to block the API call so that the correct status is displayed after the command is run.	3	23.2.0
35547941	CDCS pipeline Upgrade OCCNE.	When an exception is thrown on stage 1 of the upgrade procedure, the process continues, and it does not stop until it reaches stage 2.	3	23.2.0
354474476	CDCS upgrade fails for 23.2.0	When upgrading CDCS and a new Jenkins release is required, that release is not being downloaded to CDCS during upgrade.	3	23.2.0

Table 4-6 (Cont.) CDCS 23.2.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35653383	OCCNE upgrade marked as error because pods are in terminating state	OCCNE upgrade is marked as failed (even when upgrade script is run successfully) as some pods are in terminating state.	3	23.2.0

Note:

Resolved bugs from 22.4.1, 23.1.0, and 23.1.1 have been forward ported to release 23.2.1.

Table 4-7 CDCS 23.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35323879	NF pipeline job used in NF rollback for SCP failed with the timeout error.	SCP rollback using CDCS failed due to a timeout error. The actual rollback process requires about 20 minutes, but the rollback pipeline only affords a timeout value of five minutes, triggering a failure.	3	22.4.1
35372347	Numeric character is not allowed in username.	CDCS reported an invalid user account name error message while entering a username starting with a numeric character in managing staging sites.	3	23.1.0
35449885	CNE upgrade fails when OpenStack password contains a percent symbol.	The Upgrade CNE pipeline failed for CNE 23.1 upgrade when the openstack authentication password contains % (percentage), therefore, an upgrade of CNE is not possible.	3	• 23.1.0 • 23.1.1
35450060	LDAP deactivation does not list cdcs_internal user.	If the user enables the LDAP feature and then disables it, the cdcs_internal user cannot be used.	3	23.1.0

Table 4-7 (Cont.) CDCS 23.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35449977	LDAP feature activation failure causes future feature attempts to fail.	When the user's initial login attempt fails and the user tries to log in again, the result says that LDAP is already enabled but the LDAP .yaml file shows the profile as null and cannot be used.	3	23.1.0

> **Note:**
>
> Resolved bugs from 22.4.1, 23.1.0, and 23.1.1 have been forward ported to Release 23.2.0.

4.2.3 CNC Console Resolved Bugs

CNC Console 23.2.2

There are no resolved bugs in this release.

Table 4-8 CNC Console 23.2.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35811938	CNCC Upgrade from 23.1.1 to 23.2.0 Fails with Readiness Probe Failure	The user was not able to upgrade from CNC Console version 23.1.1 to 23.2.0 because of a PodDisruptionBudget version mismatch error. The CNC Console Helm chart was updated to resolve this issue.	2	23.2.0

Table 4-9 CNC Console 23.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35321730	PUT request is not working for MappingOfNssai	NSSF PUT request URI was not appended with the passed query parameter in the CNC Console UI.	3	23.1.1

Table 4-9 (Cont.) CNC Console 23.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35072313	After upgrade from CNCC 22.3.0 to 22.4.0, NF (PCF with 22.3.2) , CNCC prompt the configuration as No Content Found for all the services.	A "No Content Found" error was observed when CNC Console was deployed with ASM enabled. As a resolution, a workaround has been documented in the CNC Console Troubleshooting Guide where the user can create a PeerAuthentication for CNC Console namespace and disable ASM-MLTS. This workaround is only applicable for lab setups and is not recommended for production environments.	3	22.4.0
35192974	Unable to select instance on subsequent CNCC logins	The user was redirected to the Policy section when they logged in to CNC Console for the second time. They were unable to change from Policy to Common Services without clearing cache and cookies. As a workaround, the user could open a new browser window, however, the issue was resolved as part of CNC Console 23.2.0.	3	22.4.1

Note:

Resolved bugs from 23.1.x and 22.4.x have been forward ported to Release 23.2.0.

4.2.4 cnDBTier Resolved Bugs

Table 4-10 cnDBTier 23.2.5 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36042293	PCF W2 - ndbmtd pods restarted	cnDBTier required the following updates: • Update to accommodate AWS EFS file system limitation. • MySQL cluster change to ignore ENOENT error from the `unlink()` system call.	2	23.2.1
36419377	ndbmysqld pods are not getting upgraded from 23.4.2 to 24.1.0-rc.5 DBtier version on ASM setup without replication and without TLS case	Replication SQL pod count had to be set to "0" for standalone cnDBTier cluster to avoid upgrade issues in ndbmysqld pods.	3	24.1.0
35657461	Multiple restarts observed in ndbmysqld pods during upgrade to 23.2.1	When aspen mesh service was enabled, the replication SQL pod restarted before it came up and connected to the cluster.	3	23.2.1

Table 4-11 cnDBTier 23.2.4 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
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 4-11 (Cont.) cnDBTier 23.2.4 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
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	Whe SSH connection is 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
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
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
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
36146937	cnDBTIer 23.4.0 - DR Guide Refinement Request: 7.4.9.1 Procedure Point 2.d	The steps to retrieve 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 4-12 cnDBTier 23.2.3 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35956435	Cluster failure on Mansfield Voice PCF	cnDBTier cluster failed due to a change in the order in which database heartbeats are transmitted.	1	23.2.1
35956635	Geo-Replication Recovery failed in a 4 site setup with 1 other site FAILED	Georeplication recovery was stuck in the `BACKUPRESTORE` state and then in the `RECONFIGURE` state, resulting in georeplication recovery failure in a four site setup.	2	23.2.1
35899529	PCF is not sending N28 or N36	Database replication service failed to restart the ndbappmysqld pods after the georeplication recovery was complete.	2	23.1.3
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
36012733	DR procedure failed	The backup initiate REST API took more than 10 seconds to respond leading to fault recovery failure.	3	23.1.2
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
35906173	Timeout observed in Upgrade during Horizontal scaling procedure of ndbappmsyqld pods.	The Helm upgrade timed out when the upgrade was run simultaneously along with ndbappmysqld auto-scaling.	3	23.3.0
36017914	Update the default namespace in occndbtier_grafana_promha_dashboard_23.2.3-rc.1.json	The default namespace value in Grafana dashboard had to be updated from samar1 to .* (dot star).	4	23.2.3
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 4-12 (Cont.) cnDBTier 23.2.3 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

Table 4-13 cnDBTier 23.2.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35410102	DR failure due to error : remotesitedatanodecount.properties does not exists	/var/occnedb/dbbackup/remotesitedatanodecount.properties got removed if 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	PVC monitoring increased the PVC load in cnDBTier due to which the ndbmtd pods went into the crashLoopBackoff status after the deployment.	2	23.2.0
35677152	DR Stuck in INITIATEBACKUP; Failed to create a file, filename: backup_encryption_password	Fault recovery got stuck in the INITIATEBACKUP state and failed to create the backup_encryption_password file.	2	23.2.1
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
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

Table 4-13 (Cont.) cnDBTier 23.2.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35643518	Channel switchover leading to replication break on multi channel setup	Due to network delays, switchover failed to resume in case of rest API timeout.	2	23.2.1
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 cnDBTier code.	2	22.4.3
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
35561614	DBTier 23.2.0 high number of writes when Inframonitor PVC Health Enabled	High disk writes were observed when the PVC monitoring feature was enabled. That is the PVC Monitoring feature increased the PVC load in cnDBTier.	3	23.2.0
35711068	22.4.3 Vertical Scaling of ndbappmysqld pods has nothing for its PVC	Oracle Communications Cloud Native Core, cnDBTier User Guide needed to be updated with the PVC vertical scaling procedure for ndbappmysqld.	3	22.4.3
34997129	Clarification on DBTier Automated Backup behavior	The time zone of db-backup-manager-svc and db-backup-executor-svc needed to be changed to the UTC format.	3	22.4.0

Table 4-13 (Cont.) cnDBTier 23.2.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
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
35590372	cnDBTier 23.2.0 MIBs and alertrules don't match	The MIBs in cnDBTier 23.2.0 and alert rules didn't match.	3	23.2.0
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
35395995	Alert BINLOG_STORAGE_FULL since installing 22.3.2	BINLOG_STORAGE_FULL alert was raised when apiReplicaCount is 0 and replication SQL PCV is set to zero.	3	22.3.1
35364251	DBTier 22.4.1 alert's expression issues	The REPLICATION_SWITCHOVER_DUE_CLUSTERDISCONNECT alert needed to be cleared after a fixed time.	3	22.4.1

Table 4-13 (Cont.) cnDBTier 23.2.2 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
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
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 CSAR package was incorrect.	3	23.2.1
35667464	Correct panel locations for Infra Health Monitor Metrics	PVC monitoring Grafana dashboards were placed in incorrect locations.	4	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
35569579	File name should be updated in 23.2.0 Post Install Guide	The Grafana and Alert file names in *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide* needed to be corrected.	4	23.2.0

Table 4-14 cnDBTier 23.2.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35097185	During CNDB upgrade from 22.1.1 to 22.2.5, multiple restarts can be observed in CNDB pods.	Backup manager service pods restarted multiple times during an upgrade. This is a normal behavior observed when the backup manager service encounters an error. Therefore, cnDBTier documents are updated with notes regarding self restarts of backup manager service in case of errors.	1	22.2.5
35125409	Replication breaks and same error observed in ndbmysql pod in two scenarios - MTA feature is not working	Replication broke on the cnDBTier setups where the MTA feature was enabled. It was identified that MTA feature was causing the replication issue. Therefore, the MTA is temporarily disabled.	2	23.1.0
34618463	Horizontal Scaling of ndbmtd pods	The horizontal scaling of ndbmtd pods procedure in the cnDBTier user guide required updates regarding the sequence to be followed while creating node groups.	2	22.3.0
35523597	cnDBTier MoP Updates:steps for ndbappmysql pod scaling with service accout and autoscaling disabled	cnDBTier user guide was missing steps to horizontally scale ndbappmysqld when autoscaling is disabled.	3	23.1.1
35494876	SQL pods stuck in crashloop on cndb 23.2.0 after restore with backup taken on 22.4.1	cnDBTier backup and restore were not supported for different cnDBTier versions.	3	23.2.0
35202648	DR Guide Refinement Request, re: 4-Site Geo-Replication	Fault recovery procedures in the cnDBTier Fault Recovery Guide required certain refinements and additional information.	3	22.4.1
35249321	Automatically purge some binlog on startup if it is full to avoid pod going in crashloopbackoff state	The binlog files were not automatically purged on startup. This caused the binlog to overflow leading to replication failures.	3	22.4.1

Table 4-14 (Cont.) cnDBTier 23.2.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35524871	DBTier password Change Procedure Failed	The dbtpasswd script required specific updates to run in the customer environment.	3	23.1.1
35116989	DBTier MIB does not comply with standard RFC2578	cnDBTier MIB did not comply with the RFC2578 standard.	3	22.4.1
35526956	Metric for db-infra-monitor svc not documented in User Guide	Request to create and document metrics and alerts related to PVC health monitoring.	3	23.2.0
35527785	mksecrets.sh script name is mentioned wrongly in the cnDBTier installation guide,	The mksecrets.sh script name was incorrect in cnDBTier Installation, Upgrade, and Fault Recovery Guide.	4	23.2.0

Table 4-15 cnDBTier 23.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35208871	Binary log cache data overflowed to disk 577 time(s) observed in sql logs	cnDBTier liveness probes used the root password to query the database on mysqld pods. Due to this, when the root password was changed, the liveness probe failed and the pods restarted.	1	23.1.0
35194625	Data loss observed along with 'Binary log cache data overflowed to disk 577 time(s). Consider increasing --binlog-cache-size' error in sql logs	cnDBTier liveness probes used the root password to query the database on mysqld pods. Due to this, when the root password was changed, the liveness probe failed and the pods restarted.	1	23.1.0
35139386	During CNDB upgrade from 22.4.1 to 23.1.0, multiple restarts can be observed in ndbmysql pods	Multiple restarts were observed in ndbmysqld pods during an upgrade.	1	23.1.0
35274059	VALIDATION WARNING: 1 WARNINGS FOUND	Multiple restarts were observed in ndbmysqld pods during an upgrade.	1	23.1.1
35125409	Replication breaks and same error observed in ndbmysql pod in two scenarios - MTA feature is not working	Replication broke on MTA-enabled setups. This resulted in temporarily disabling the MTA feature.	2	23.1.0

Table 4-15 (Cont.) cnDBTier 23.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35260142	Replication not working post upgrade using vCNEEgress feature	Replication was not working as egress annotations were added to services and not the deployments. Egress annotation is modified to add the annotations to deployments instead of services to resolve this issue.	2	23.1.0
35323629	Unable to run disaster Recovery on a TLS and HTTPS enabled setup	Georeplication restore process was not running on a cnDBTier setup where HTTPS was enabled.	2	23.1.1
35348712	ndbmtd scaling procedure taking more than 20 min time for restarting the geo replication sql pods	ndbmtd scaling procedure was not working as cnDBTier pods took more time to come up, when data pods were added before restarting all cnDBTier pods.	2	22.3.0
35365647	Prod Sm PCF Active session went down to 0 during upgrade 22.4.5 in CLSP	ndbmtd scaling procedure was not working as cnDBTier pods took more time to come up, when data pods were added before restarting all cnDBTier pods.	2	22.4.5
34618463	DBTier_FT_MC: Horizontal Scaling of ndbmtd pods	ndbmtd scaling procedure was not working as cnDBTier pods took more time to come up, when data pods were added before restarting all cnDBTier pods.	2	22.4.2
35268598	Rollback from 23.1.0 to 22.4.1 failed for TLS enabled Cndb setup	Rollback procedures failed on cnDBTier sites where TLS was enabled.	2	23.1.0
35116989	DBTier MIB does not comply with standard RFC2578	cnDBTier MIBs did not comply with the RFC2578 standard. As a result, cnDBTier MIBs failed during the compilation process.	3	22.4.1

Table 4-15 (Cont.) cnDBTier 23.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35290030	Replication service (Failed Site) pod restart is needed to make DR work if the previous DR has been failed	DB backup executor service was unable to compress the backup files when the disk was not available. As a result, the fault recovery process failed.	3	22.4.1
35290005	Backup getting processed even if the PVC doesnt have enough space during DR	DB backup executor service was unable to compress the backup files when the disk was not available. As a result, the fault recovery process failed.	3	22.4.1
35249321	Automatically purge some binlog on startup if it is full to avoid pod going in crashloopbackoff state	The delta binary logs were not purged automatically during the startup when PVC was full. This caused the pod to go into the crashloopbackoff state.	3	22.4.1
35335531	GR state is retained as "COMPLETED" when DR is re-triggered	When a site is marked as failed, the georeplication state (gr_state) of DBTIER_REPL_SITE_INFO must be updated to NONE or NA. But, gr_state was retained as COMPLETED.	3	23.1.1
35297883	Response body of DB Tier Backup APIs for 500 error code should be made generic	The user requested to generalize the response body (error messages) of 500 error codes in cnDBTier Backup APIs.	4	23.1.1
35372410	Correction needed in spelling in replication svc logging	There was a typo in the replication service log message.	4	23.1.1

Note:

Resolved bugs from 22.3.4, 22.4.5, and 23.1.1 have been forward ported to Release 23.2.0.

4.2.5 CNE Resolved Bugs

Table 4-16 CNE 23.2.6 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35369547	Target index not getting deleted as part of ILM	When a targeted index is 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
36125787	OCCNE 23.2.5 Issue in adding new lbvm in vCNE	While adding a new pair of Load Balancer Virtual Machines (LBVM) to vCNE in an OpenStack environament, the `lbCtrlData.json` file populated by `./scripts/addPeerAddrPools.py` was incorrect.	2	23.2.5
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 4-17 CNE 23.2.5 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 23.2.3 to 23.2.4 failed due to multiple reasons.	3	23.2.4

Table 4-18 CNE 23.2.4 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35857501	CNE 23.2.1 LBVM's lb_monitor.py not monitoring failures due to "UPGRADE_IN_PROGRESS=False" env variable set in lb-controller pod	Pausing or stopping the active LBVM did not result in a switchover or failure detection in lb-controller.	2	23.2.1

Table 4-19 CNE 23.2.3 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35674438	vCNE install on openstack for 23.2.0 has failed	vCNE 23.2.0 on OpenStack installation attempt failed with istio test failures in preproduction environment.	1	23.2.0
35729483	CNE installs has pod resource tuning settings for opensearch/ elasticsearch, and some PVC tuning that can be done via occne.ini file for openstack.	The user needed more information on how to tune the CPU, RAM resources of other pods, except opensearch, to override the default resources assigned by CNE. This was already documented in *Oracle Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide*.	3	23.2.1

Table 4-20 CNE 23.2.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35471163	removeBmWorkerNode.py does not completely remove a BM node	While running the script to automatically remove Kubernetes worker node in a Bare Metal cluster, the script was not performing the following actions: • Logging to an external file (removeBmWkrNodeCapture-${DATE}.log) was not called. • While removing the OSD, the script left a phantom negative ID related to the removed node. This ID was not completely removed.	3	• 23.1.1 • 23.2.0
35307224	Complete switchover didn't happen after replication LBVM failure	The `boot.log` file in the `/var/log` directory of the LBVM was filled by logs generated by a python script and was not getting rotated. This resulted in the LBVM disk space getting full which subsequently led to a LBVM failure.	3	• 23.1.1 • 23.2.0

Table 4-21 CNE 23.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35168065	High CPU usage on CNE 22.4.1 nodes	High CPU usage was observed on CNE 22.4.1 nodes.	2	22.4.1
35026633	CNE 1.10.3 lb-controller kubectl certificates not updated with OCCNE API certificate renewal	lb-controller kubectl certificates were not updated with CNE API certificate renewal process.	2	1.10.3

Table 4-21 (Cont.) CNE 23.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35089494	Opensearch Index Management Operations are not working	Index management lifecycle was failing: OpenSearch Index Management operations were failing, indexes were not transitioning from hot to warm state, force merge was not working for any indexes, and delete was not working.	2	23.1.0
35061535	OpenSearch GUI doesn't show complete SCP log	FluentBit stalled to ingest data in OpenSearch. On investigating the issue, it was found that the OpenSearch index creation process blocked ingestion of API calls when the cluster observed high disk usage or high compute usage.	2	23.1.0
34978552	After Upgrade to 22.3 VMware LBs are left with dysfunctional ifcfg file	After an upgrade, LBVMs were not functional due to a configuration that was not applied during the automation.	2	22.4.0
35182156	LBVMs unable to communicate with backend services	The user requested to combine the `k8s` and `k8s-node` security groups that are applied to worker nodes.	2	22.4.1
35399559	Issue with very high cpu usage for Egress controller pods	High CPU usage was observed in Egress controller pods.	3	• 22.4.1 • 22.4.2 • 22.4.3
35339676	sync_bastions script design has permissions issues that will break syncronization in multiple scenarios	The Bastion registry was run as root. This led to problems with rsync cron job in some cases where a root created registry image was required to be deleted after a switchover.	3	• 22.4.1 • 22.4.2 • 23.1.0 • 23.1.1
35334779	sync_bastions script creates duplicated keys within known_hosts file	The `sync_bastions` script created duplicate SSH key entries in the `known_hosts` file on Bastion Hosts. As this file grew in size, SSH logins began to slow down noticeably.	3	• 22.4.1 • 23.1.0 • 23.1.1

Table 4-21 (Cont.) CNE 23.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34686444	Both LBVMs for a service going down at the same time corrupts the SQL database on the lb-controller	The SQL database, containing the information about active and standby LBVMs for a particular service, was populated with FAILED entries.	3	• 1.10.3 • 22.4.0

> **Note:**
>
> Resolved bugs from 22.3.3, 22.4.3, and 23.1.1 have been forward ported to Release 23.2.0.

OSO 23.2.0

There are no resolved bugs in this release.

4.2.6 NEF Resolved Bugs

Release NEF 23.2.1

Table 4-22 NEF 23.2.1 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	When upgrading, NEF replication break was observed. Even though Site1-CNDB1 ndbmysqld-1 pod restarted one time, it is not recovered after the replication break.	1	23.2.0
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	23.2.0
35763438	TI subscription with External Group ID is giving error as "Routing Rule not found"	TI subscriptions that includes an External Group ID were receiving the following error: **Routing Rule not found**	3	23.2.0

Release NEF 23.2.0

Table 4-23 NEF 23.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35202851	During In-service upgrade, the failure rate is 1.3% and also there is complete loss in traffic for few seconds	While upgrading in-service, the failure rate was 1.3%, and there was complete loss in traffic for few seconds.	2	23.1.0
35272352	During in-service solution upgrade of NEF, traffic loss is 2.16% during cndb upgrade	While in-service upgrade for NEF, traffic loss was 2.16% for cnDBTier upgrade.	2	23.1.0
35311135	Incorrect format of 3gpp-sbi-discovery-service-names in header when there is multiple services	When there are multiple services, the user found the incorrect format of 3gpp-sbi-discovery-service-names in header.	2	23.1.0
35396840	5gc agent pod is not coming up if we add (TI parameters :geoZoneId) in yaml file and upgrade	When Technical Indicator (TI) parameters were set to geoZoneId in the yaml file, then the 5GC Agent pod did not come up after the upgrade.	3	23.1.0

Note:

Resolved bugs from 23.1.x have been forward ported to Release 23.2.0.

4.2.7 NRF Resolved Bugs

NRF 23.2.3 Resolved Bugs

Table 4-24 NRF 23.2.3 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
36215531	NRF Rejecting discovery when “allowedPlmns” does not contain the PLMN in registration profile	The PLMN ID(s) registered in the NF profile were not considered while accessing the NF service instance when the allowedPlmns attribute is present at the NFservice level.	2	23.2.1
36194956	NRF 23.1.2: OcnrfOverloadThreshold BreachedL1 alert raised in production site	NRF's AccessToken service reported invalid pending message count due to which overload alert was raised and did not clear.	3	23.1.3

Table 4-24 (Cont.) NRF 23.2.3 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
36215468	Logs are incorrectly getting reported as ERROR causing flooding of logs in NRF 23.2.2 Discovery pods.	Incorrect logs were generated when target nftype is UDR, UDM, or any NF type that contains SUPI as query parameter. The logs were flooding in the discovery pods, which might exhaust the ephemeral storage of the pod leading to downtime of these pods.	3	23.2.2
36215718	ocnrf_replication_status _total does not get pegged on nrfArtisan service	ocnrf_replication_status _check_total did not get scraped from the artisan pod due to which OcnrfReplicationStatus MonitoringInactive alert was raised for the pod even if replication is up.	3	22.3.2
36215805	indentation issue as whitespace character got substituted by tab unintentionally - broke yaml lint	Upgrade or rollback failed with the yaml lint error. This was because of the indentation issue.	3	23.2.2
36213094	NRF is not updating NFServiceListMap in case priority is getting updated in NFService level during preferred locality features	When extended preferred locality feature updates the priority or load of the profiles as per the configuration, NRF only updated the priority present in nfService attribute of the profile. The nfServiceListMap attribute was sent as it was received during registration.	3	23.2.2
36215609	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

NRF 23.2.2 Resolved Bugs

Table 4-25 NRF 23.2.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
35874824	Regression test failed on Alert12_slfDiscoveredMode	Test case failed due to timing issues between the discovery request and the artisan service updating the slfCandidateList from the registered UDR profiles. The artisan service updates the slfCandidateList, overwriting the configuration set as part of the test case, before the discovery request can be sent. The test case passes if the discovery request is sent before the artisan service refreshes the slfCandidateList.	3	23.2.0

NRF 23.2.1 Resolved Bugs

Table 4-26 NRF 23.2.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
35751693	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
35773711	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
35773733	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

Table 4-26 (Cont.) NRF 23.2.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
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
35773766	Network Policy - Add policy for CNCC and Notifications from OCNRF	Network Policy must include policy for CNCC and notifications from NRF.	3	22.4.0
35773797	NRF is taking value from user agent header rather from Access Token request json	While processing AccessToken request, NRF considered the roaming scenario based on the User-Agent Header value instead of Access Token request json.	3	23.1.0
35773856	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
35773868	NRF responding with 200 OK constantly for Heartbeat 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
35773889	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
35773574	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

Table 4-26 (Cont.) NRF 23.2.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
35829417	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
35773914	NRF 23.1.1 closing active TCP connections after 2 mins	NRF 23.1.1 was closing the active TCP connections after 2 minutes.	2	23.1.1
35829221	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
35829429	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
35829440	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
35830327	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
35830341	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

Table 4-26 (Cont.) NRF 23.2.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
35768970	UDM patch request to update "serviceInstanceId" gets rejected by NRF	UDM sent a Patch request to update "serviceInstanceId" as the pod name of their LB pod with serviceName as prefix, and UDM tried to update this serviceInstanceId whenever its LB restarted.	2	23.2.0
35781885	Incorrect x5c header type(string) in jwt token implemented for NRF feature CCA Header Validation	Incorrect type (string) x5c header value in jwt token was implemented for CCA Header Validation feature.	2	23.2.0

Table 4-27 NRF 23.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
35314965	NRF not sending mateScpInfoList in profile retrieval 23.1.0	NRF was not sending mateScpInfoList in profile retrieval when mateScpInfoList was empty in customInfo.	2	23.1.0
35286843	Error code 503 is observed across all NRF operations during 12K TPS performance run on each site	Error code 503 around 0.01% was observed across all NRF operations during 12K TPS performance run on each site.	2	23.1.0
35291189	OCNRF 23.1.0 Upgrade from 22.4.0 fails with "unknown anchor 'imagePullPolicy' referenced"	Upgrade from 22.4.0 to 23.1.0 was failing with the error: unknown anchor 'imagePullPolicy' referenced. This error was raised for ocdebug-tools.	2	23.1.0
35417911	InterPlmnFQDN is coming in NFServiceList attribute during Discovery Response	When NRF was sending a discovery response, InterPlmnFQDN is coming in NFServiceList attribute. InterPlmnFQDN must not be present in the discovery response.	3	23.1.1
35417836	Network Policy is not allowing connections from different namespace	Network Policy was not allowing connections from different namespace of NRF towards NRF Ingress Gateway.	3	23.1.1

Table 4-27 (Cont.) NRF 23.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
35417814	Discovery Cache is not refreshing records for Custom NFs	NRF wasreturning older NfProfile in the NfDiscovery response for custom NFs. NRF discovery micorservice cache is not getting refreshed for custom NFs.	3	23.1.1
35417896	SLF error metrics are not pegged when decoding response fails	SLF error metrics were not getting pegged when decoding of SLF response failed.	3	23.1.1
34617800	MessageCopy feature in NRF not displaying GZIP format logs	MessageCopy feature in NRF does not support GZIP format logs.	3	22.3.0
35116837	REST API State Data Retrieval of subscription query param nf-status-notification-uri FAILED	subscription-details API was not filtering as expected based on the query parameter, nf-status-notification-uri, and giving all non-matching results.	3	23.1.1
35250486	Value of Discovery response in Grafana for Discovery microservice is indicating incorrect value	The forwarded responses were not included in the overall discovery response metric, ocnrf_nfDiscover_tx_responses.	3	23.1.0
35290341	Add missing test case for reroute mechanism on delayed responses	NRF-ATS suite did not have test cases for reroute mechanism on delayed responses.	3	22.3.2
35417847	ImagePullPolicy is not being picked for App-Info micro-service	ImagePullPolicy value was not correctly picked for App-Info microservice.	4	22.4.0
34568810	CNCC NRF GUI - Help links are not working	CNCC NRF GUI had Help option that is not working.	4	1.15.0
34812893	ocnrf.active.registrations .count metric is providing incorrect values of registered NFs	ocnrf.active.registrations .count metric must not consider stale records for pegging.	4	22.1.4

Note:

Resolved bugs from 22.4.1 have been forward ported to Release 23.2.0.

4.2.8 NSSF Resolved Bugs

Table 4-28 NSSF 23.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35052433	NSSF is not sending subscription request message after timer-expiry	After configuring the `renewalTimeBeforeExpiry=60` parameter in the ocnssf_custom_values.yaml file, while adding the Amf-set in CNC Console, NSSF sends a discovery message to NRF to get all active AMFs in an AMF-set. Here, NSSF should send the subscription request to NRF for configured Amf-set. Also, NSSF should renew the subscription request after 60 seconds, but NSSF is not sending the subscription request after 60 seconds.	2	22.4.2
35114407	10K TPS has glitches when ASM/mTLS is enabled on dbtier	NSSF must support 10K TPS with ASM. However, NSSF currently supports 10K TPS with the following setup: • With ASM on NSSF and wihtout ASM on cnDBTier • Without ASM • ASM on NSSF and cnDBTier with the following annotation: `traffic.sidecar.istio.io/excludeOutboundPorts: "3306"`	2	23.1.0
35149048	NSSF ATS 23.1.0: unable to configure pipeline.	To trigger a build, the users initially needed to change some parameters in the pipeline and save, but they were unable to save the changed configuration. After selecting the save option, the user was getting HTTP 403 error.	2	23.1.0

Table 4-28 (Cont.) NSSF 23.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35273531	Operator configured data should not deleted and added while ns-availability update received from AMF	Operator-configured data should not be deleted and added in nss_rule and nssai_auth using ns-availability update requests.	2	23.1.0
35322832	25% traffic dropped observed for NS Selection procedures during in service rollback procedure from NSSF version 23.1.1 to 23.1.0	It was observed that 25% traffic was dropped for NsSelection procedures during in-service rollback from version 23.1.1 to 23.1.0.	2	23.1.1
35292858	NS Selection procedure Success rate dropped (20%) and http error 500 occurred during In service upgrade from NSSF version 23.1.0 to 23.1.1	NsSelection procedure success rate dropped by 20% and HTTP error 500 occurred during the in-service upgrade from version 23.1.0 to 23.1.1.	2	23.1.1
35328630	NSSF NsConfig request to NrfClient to discover AMFs in AMF-set is failing	After enabling `nrf.subscription` in the ocnssf_custom_values.yaml file, the user noticed that NSSF was not sending subscription requests for any AMF set configured.	2	23.1.0
35337655	In Notification, NSSF is sending invalid / OC_Notify/nssai-availability/subscriptions URL in Notification URL	The user was getting / OC_Notify/nssai-availability/subscriptions URL in Notification URL, which was not mentioned in 3GPP 29.531. Because of the Invalid URL, AMF was not receiving any notifications.	2	23.1.0
35322862	Success rate drooped 35% during In service rollback for NSSF from Version 23.1.1 to 23.1.0 for Ingress	The success rate dropped by 35% during the in-service rollback from version 23.1.1 to 23.1.0 for the Ingress pod.	2	23.1.1
35292961	Ingress failure observed during In service upgrade from NSSF version 23.1.0 to 23.1.1	Ingress failure was observed during the in-service solution upgrade from NSSF version 23.1.0 to 23.1.1.	2	23.1.1

Table 4-28 (Cont.) NSSF 23.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35218657	422 UNPROCESSABLE_ENTITY - when a specific third-party AMF sends a huge nnssf-nssaiavailability request	The user was running a test between a third-party AMF and NSSF 23.1.0. Testing nnssf-nssaiavailability service triggered a scenario where AMF was providing information about supportedNssaiAvailabilityData that consisted of 1500 TACs distributed in 75 gNodesBs (20 per gNodeB).	2	23.1.0
34874721	NSSF ATS 22.3.0 Health check failure	The health check test in ATS was failing for release 22.3.0.	3	22.3.0
35250829	The "serviceAccountName" parameter missing in ATS values yaml file	There was a request to add the "serviceAccountName" in the ocats yaml (values.yaml) file so that the installation can use the already existing service account in the lab.	3	22.4.3
35195268	Issue with the NSSF ATS deployment.yaml file	The following issues were reported for the NSSF ATS package with PVC enabled: • NSSF-ATS 23.1.0: ocnrf_tests folder was present in NSSF ATS pod. While only ocnssf_tests folder was expected in the ATS pod, an extra folder named ocnrf_tests was also present. • Wrong heading of ATS version in NSSF ATS GUI • There is an error inside the tgz files present in ocnssf_tests folder in the ATS pod.	3	23.1.0

Table 4-28 (Cont.) NSSF 23.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35266672	NSSF - Documentation error causing helm test failure	The documentation of ocnssf-resource-template.yaml had discrepancies compared to ocnssf-rbac.yaml. For example, the ocnssf_role had additional resources and verbs in ocnssf-rbac.yaml file.	3	23.1.0
35209131	Error 422 occurred for procedure "avail-patch" during traffic run with 2.5K TPS NSSF	Error 422 occurred for procedure "avail-patch" during a traffic run with 2.5K TPS. NSSF Avail patch (add and remove) experienced failure with error code 422.	3	23.1.0
35138414	For Same AMF-ID, SNSSAI, MCC, MNC and TAC NsAvailability PUT is not working for other sites	For the same AMF-ID, SNSSAI, MCC, MNC, and TAC NsAvailability, PUT was not working for other sites.	3	23.1.0
35138363	NSAvailabality Delete is not working in GR Setup	While running performance in GR Setup for consecutively running NsAvailability PUT, NsAvailabalityDelete, and again NsAvalabality PUT, it was showing an error for duplicate entry in NsAvailabalityData table.	3	23.1.0
35178788	Success rate dropped and internal server error occurred in Ingress pod while running traffic with 2.5K TPS on Debug Build	The success rate dropped and an internal server error occurred in the Ingress pod while running traffic with 2.5K TPS.	3	23.1.0
35191414	PV parameters are not present in ATS values.yaml	PV parameters were missing from the ATS values.yaml file.	3	23.1.0
35191006	Subscription-Patch-Unsubscription is not working in 3 site GR Setup	After applying the patch 23.1.0, POST Nssai Subscription was throwing an error in a three site GR setup.	3	23.1.0
35174619	Issue with Availabilty put in 3-site GR setup	While running ns-availability-put traffic on different sites, the user was getting duplicate entries for the key.	3	23.1.0

Table 4-28 (Cont.) NSSF 23.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35149397	NSSF ATS 23.1.0: GR_NSAvailability_PUT is getting failed	GR_NSAvailability_PUT feature was failing in the regression pipeline. In the previous version of NSSF 22.4.2, this feature was present in the New Feature list and it passed back then.	3	23.1.0
35052539	NSSF is not sending the expected data for log level	CNCC UI was not showing any default log level for all NSSF services.	3	22.4.2
35188822	In amf_tai_snssai_map table, amf_set_id is incorrect format while using amf_id present in amf_resolution table.	In the amf_tai_snssai_map table, amf_set_id was shown in an incorrect format while using amf_id present in the amf_set and amf_resolution table.	3	23.1.0
35095820	IN NSI Profile, NRF Access Token URI is mandatory parameter in CNCC UI	In CNC Console UI, NSSF, NSI Profile, and Add the New option, an error was showing in the inspect tab. Also, NRF Access Token URI should be mandatory in CNC Console UI.	3	22.4.2
35259920	While running 10k traffic with at NSSF with ASM 503 responses are being observed	While running 10k traffic at NSSF with ASM, 503 responses were observed.	3	23.1.0
35022513	NSSF is sending incorrect targetNfType in discovery message towards NRF	NSSF was sending incorrect targetNfType discovery messages to NRF.	3	22.4.2
35265168	In GR scenarios NsAvailability PUT on site1 and PATCH on Site2 not working	An error log was observed after enabling DEBUG on a 3-site GR setup.	3	23.1.0
35174548	OCNSSF should reject the NSAvailability delete request if NFId (NSSAI availability information) is unavailable	AMF deleted an already existing S-NSSAIs per TA provided by the NF service consumer (for example, AMF).	3	23.1.0

Table 4-28 (Cont.) NSSF 23.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35288594	NSSF should reject the ns-availability update request when taiList IE included same value of TAI contained in the tai IE.	As per 3gpp 29.531 section 6.2.6.2.3, the taiList IE should not include the TAI contained in the TAI IE. However, the TAC is present in TAI IE and taiList IE. Because of this NSSF should reject the ns-availability update request and send a failure response to AMF.	3	23.1.0
35307504	MappingOfNssai Configuration is not displaying in CNCC UI	In CNC Console 23.1.0, MappingOfNssai Configuration was not displayed.	3	23.1.0
35285483	Not able to change the loglevel for nrf-client-discovery and nrf-client-management through CNCC	There was no option to set LogLevel in ocnssf_custom_values.yaml for nrf-client-discovery and nrf-client-managemen microservices. An update in the ocnssf_custom_values.yaml file was required to add the log level. From CNC Console, it was neither able to fetch the current log level nor able to change it. An error was observed in the CNCC while updating the log level.	3	23.1.0
35261720	NSSF - namespace name is hardcoded in the nssf-alert-rules.yaml	The namespace value was hardcoded in the ocnssf_alert_rules.yaml file. There were multiple entries of the hardcoded namespace value “ocnssf”, where the user needed to edit each instance before deployment in any environment.	3	22.4.3
35341507	After deleted all configuration, ns-availability update delete, one record is persist in snssai_list table	The record in snssai_list table was incorrect.	3	23.1.0

Table 4-28 (Cont.) NSSF 23.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35349469	If AMF is not sending the subscribedNssai parameter in ns-selection registration request, NSSF is not sending valid reason	NSSF should send valid reason such as subscribedNssai is not present in received request.	3	23.1.0
35125397	while deleting the AMF-Set, dependant NSI profile has automatically deleted the PLMN and target AMF Set.	The user configured the Amf-set and NSI Profile with the same target AMF-set that NSI Profile has configured in NSS Rule. When the user deleted the NSI Profile, it was not deleted because the NSI profile was referred the in NSS Rule. The same should be applied to NSI Profile and AMF Set configuration. AMF Set is referring to NSI Profile. If the user deletes the Amf-set, NSSF deletes the target AMF-Set and PLMN configuration in NSI Profile. This is not correct behavior for the end user. Since AMF Set is referring to NSI Profile. If AMF-Set is mapped to any NSI Profile, NSSF should send a failure notification.	3	22.4.2
35273268	5 digit tac "10001" has configured in nssai_auth but not configured in nss_rule	The user enabled nrf.subscription in the ocnssf_custom_values.yaml file but noticed NSSF was not sending subscription requests for any AMF set configured.	3	23.1.0
35322662	NSSF should validate complete array of tacRangeList (starttac, endtac) then insert any correct tacRangeList in NSSF Database.	If AMF sent multiple tagRangeList in ns-availability update request: • The first tagRangeList was no correct. The starttac range was greater than the endtac range. • The second tagRangeList was in the correct format.	3	23.1.0

Table 4-28 (Cont.) NSSF 23.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35279212	NSSF 23.1 --> Availability 422 UNPROCESSABLE_ENTITY	The user was getting 422 UNPROCESSABLE_ENTITY when running an availability update. For this test, there were two different NSSAIs than those already registered in the database, but in the same TAC. This error occurred when they sent an availability with NSSAIs that belonged to the same TAC that the NSSF has registered via the configuration API.	3	23.1.0
35363551	In AMF HAndover Scneario if one site is going down the Site Id is not changing to the Leader Site in nssai_subscriptions table	In the AMF handover scenario, if one site went down, the Site Id did not change the leader site in nssai_subscriptions table.	3	23.1.0
35180218	NS selection is not providing correct information just after ns-availability update.	While running ns-selection just after ns-availability update, NsSelection did not provide the correct information.	3	23.1.0
35349659	NSSF 23.1.0: Availability update error when one of the NSSAIs has been restricted	NSSF 23.1.0: Availability update error when one of the NSSAIs has been restricted: `"status": 406, "detail": "Grant is not allowed for these Configuration parameters.",`	3	23.1.0
35373619	NSSF should reject ns-availability update request when AMF sends empty taiRangeList	If AMF sends ns-availability update request, the supportedFeature =1 and taiList or taiRangeList IEs are present, then NSSF should validate that at least one record is present because of "cardinality 1..N".	3	23.1.0

Table 4-28 (Cont.) NSSF 23.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35373441	If starttac is null in ns-availability update request then NSSF should validate the endtac should be null	NSSF should validate that the starttac and endtac are null.	3	23.1.0

35337688	In ns-availability Update request, Getting ERROR spportedNssaiAvailabilityData contains duplicate tai from NSSF.	The user was getting the below response error from NSSF:
		
		`MESSAGE - 2023-04-20T09-43-59.298 - ctxname:<TAI_RANGE_10.avail_put[ns-avail_Update_put].[CallFlow].avail-put> -`
		
		`ctxtype:<FlowStepCtx>`
		`http response received:`
		`Status: 400`
		`Method: PUT`
			3	23.1.0

35373599	NSSF should reject ns-availability subscription request when AMF sends empty taiRangeList.	If AMF sent ns-availability subscription request, the supportedFeature =1 and taiList or taiRangeList IE's were present then NSSF should validate at least one record must be present because of "cardinality 1..N".	3	23.1.0
35180629	If plmn level Profile is not configured, NS-Availability update failed in first execution after that it works as expected.	The user received an unexpected response in the following scenario:: The user was running ns-availability update without configuring PLMN Level Profile. The old configuration was deleted using curl commands and all the default configurations were performed using perfgo.	3	23.1.0

Table 4-28 (Cont.) NSSF 23.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35123768	OCNSSF send multiple unknown Headers in subscription message request towards NRF	While adding the amf-set in CNC Console UI, NSSF sends a subscription message to NRF to get all the active AMFs in an AMF-set. In this subscription message request, the user noticed multiple unknown headers.	3	23.1.0
35185702	NsAvailability is creating a duplicate subscription	NsAvailability must not create more than one entry for a Subscription. At a given site, the combination of notification URL and Tai/TaiRangeList must be unique in nssai_subscriptions table.	3	23.1.0
35382032	Unable to save "NSSF->Log Level Options" for some services, Getting Error Code: 400 Could not find the config for requested service. - BAD_REQUEST	In CNC Console for NSSF 23.1.1, the below services showed BAD_REQUEST error. • alt-route • nrf-client-nfdiscovery • nrf-client-nfmanagement • perf-info	3	23.1.1
35387502	NSSF is not processing pending eventTriggers after GR site is down	NSSF did not process pending eventTriggers when a GR site was down.	3	23.2.0
35299671	NSSF 22.4.4 : Multiple ServiceAccount Yaml file in package	Multiple yaml files were available for serviceaccount in the package. However, there should be only one file and redundant files should be removed.	3	22.4.4

Note:

Resolved bugs from 23.1.x and 22.4.x have been forward ported to Release 23.2.0.

4.2.9 Policy Resolved Bugs

Table 4-29 Policy 23.2.8 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36290600	Sy's SNRs not working when "Type of Search" is set to "Preferential Search" and GPSI in PDS Settings	Sy's SNRs were not working when "Type of Search" was set to "Preferential Search" and preferential order was set to "GPSI" in PDS Settings.	3	23.2.8
36319650	pcrf-core to PDS communication is not properly load balanced.	The communication between PCRF-Core and PDS lacked proper load balancing.	3	22.4.5

Note:

Resolved bugs from 23.2.x have been forward ported to release 23.2.8.

Table 4-30 Policy 23.2.7 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36101095	3-way call with non peer networks	In AAR-U, while updating an existing MediaComponent, the values of the rrBw and rsBw media components were not changing.	2	23.2.5
36124195	CHF connector HTTP2 Remote Reset causing N28 create failure	CHF connector was failing with concurrent modification exception during validation of SBI binding header value with NFSet while sending CHF policy counter look up request.	3	23.2.6

Note:

Resolved bugs from 23.2.x have been forward ported to release 23.2.7.

Table 4-31 Policy 23.2.6 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35969372	Initial CHF Retry Request goes to same SCP	Initial retry requests were sent to the same SCP (SCP 11) instead of the alternate SCP, even though the alternate SCP was enabled. While subsequent requests were sent to alternate SCP (SCP 12), both initial and subsequent requests were sent to alternate CHFs from NF's point of view.	3	23.2.4
35966294	Sd interface - RAR is not triggered to TDF when SNR from OCS	PCF did not initiate the RAR message towards TDF to change the ADC rule, when the Policy counter status changed in SNR message from OCS.	3	23.2.6
35934595	PCRF Export Policy not working	When doing Export Policy in CNCP GUI, it is getting stuck at 0% and Status in INIT. The export activity was not completed.	4	23.2.0
35932926	UDR connector prompting Error "Caught Exception while DELETE"	For session/ subscription clean-up towards UDR for users, the log flooded even with log level set to WARN.	4	23.2.1
35915557	Issue with exporting Policy after importing it successfully in PCF 23.2.2	After successful Policy import, Policy export was getting stuck at 0%. This issue was observed only with specific Policy export and not with complete export (config+policy).	3	23.2.2

Table 4-31 (Cont.) Policy 23.2.6 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35907336	PCF SM pods were getting flooded with "exception java.lang.NullPointerException"	After enabling the audit, the audit pods were getting flooded with below errors: `{"instant":{"epochSecond":1697186879,"nanoOfSecond":100785084}`	3	23.2.4
35901378	Topology_hiding_PCF Feature Failure in Regression	Both the scenarios of the feature Topology_hiding_PCF were failing with the following error: “Then Validate Diameter AAA-I message in recv0 from /var/lib/jenkins/ocpcf_tests/data/pcf/Topology_hiding/diamsim/Topology_hiding_SM_Rx_for_STR/aaa-i.json”	3	23.2.4
35845101	PCF not sending 3gpp-sbi-binding header in audit notification response to BSF	For SM create request, PCF sent binding create message to BSF along with 3gpp-sbi-binding header containing nfset in PCF profile. BSF sent session audit notification to PCF and PCF did not add 3gpp-sbi-binding header in the response.	2	23.2.3
35807416	Incorrect IE in ampolicy update message	AM service was sending update to AMF without invalid null parameters when there were no policy updates required.	3	23.1.7

Table 4-31 (Cont.) Policy 23.2.6 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35647226	Complete configuration to enable Pending transactions on SM Policy is not available in User guide, FDD or any other product document	Complete configuration to enable pending transactions on SM service was not available in Policy User Guide, FDD or any other product documentation. Details about the exact configuration keys and values (along with defaults) to support pending transactions and locking in Bulwark were not present in any of the product documentation for SM service. FDD included configuration details for AM service and UE Policy service. It should also include details about the advanced settings keys and values for SM service to support Bulwark locks/unlocks for SM update and SM update notify requests.	2	23.2.0
35638749	subs-to-notify is not getting triggered in SM Update if it fails while SM create	As per the feature description and call flow, if subscribe to notify request failed with 4xx/5xx error code during SM create, then during SM update process PCF should retry the subscribe to notify request towards UDR. But, PCF was not initiating subscribe to notify request towards UDR during SM update.	2	23.2.0

Table 4-31 (Cont.) Policy 23.2.6 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35339370	PROD PCF ocpm_ingress_response_total Does not show failures for UE and AM Policy	The AM/UE Policy metrics under PCF AM dashboard in Grafana did not display the failures. The failures were displayed only on the ingress gateway metric.	3	22.3.2
35962366	Sd RAR intermittent pcrf core throwing error as no peer	RAR for Sd session termination was not happening for all the CCR-T requests received from PGW.	3	23.2.4
35988964	Pending Transaction after Rx STR	SM UpdateNotify was sent when there was no AppSession information present.	3	23.2.4

Table 4-32 Policy 23.2.5 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35896637	Pending transaction retry with new rule contents	PCF updated the QoS and charging data references and did not update the new QoS/ Charging data when the pending transaction retry updateNotify was backed off for a second. Hence, SMF was responding with PCC_Rule event even if valid QoS/ Charging data was not available to SMF. And, PCF was sending Rx RAR successful resource allocation message to P-CSCF on receiving 400 pending transaction from SMF.	2	23.1.7

Note:

Resolved bugs from 23.2.4 have been forward ported to release 23.2.5.

Table 4-33 Policy 23.2.4 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35843535	Clarification on nUDR notification 400 Error in PCF 23.2.2	PCF checks the UDR connector side for the *ueId* field which cannot be null in the Notification body from the UDR.	1	23.2.2
35797403	PolicyDS profiles not being removed or updated correctly	PCF had outdated information in the pdssubscriber record referencing the pdsprofile for the subscriber.	2	22.4.5
35806918	enhancements to SM/Audit logs for debugging maxTTL issues	Whenever Audit Notification was sent to SMF and received ERROR in response, audit attempt logs did not contain the notification URL used in SM update notify and the reason for the failure (httpStatus code).	2	23.1.7
35812250	SM_Records getting deleted due to MaxTTL	Audits initiated *UpdateNotify* retries on error failed when Session retry logic with alternate route profiles was configured.	2	23.1.7
35787703	Production SM PCF IGW overload and 429 errors	Overload was triggered on Ingress Gateway when there was no change in the load and did not auto clear the condition. Also, no alert was generated for triggering this overload condition.	2	23.1.6

Table 4-33 (Cont.) Policy 23.2.4 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35427441	Different notification URI used in first and subsequent AMF retry attempt by PCF	If the notification URI was updated through UE Update when triggering a UDR notification, the initial attempt used a different URI to notify AMF. Now, the correct URI is being used to send the notification to AMF.	2	23.1.1
35511302	PCF 22.4.5 pcrf-core error with ASA (It shows error processing with DIAMTER_UNABLE_TO_COMPLY but it is receiving ASA with DIAMTER_SUCCESS)	When the PCRF core pod sent an ASA, it included both Diameter response codes in the same reply (5012 DIAMETER_UNABLE_TO_COMPLY and 2001 DIAMETER_SUCCESS). However, the Prometheus metrics only displayed Diameter 2001 and Diameter responses.	2	22.4.5
35723752	AAR being responded to with 5012 on Voice PCF	A Gx session was active, and there were no trace messages indicating an attempted RAR.	2	22.4.6
35865414	PCF PRE logs is not completely getting recorded in the Kibana	PCF's PRE logs were not fully recorded in Kibana.	2	22.4.2
35863045	PRA Status session variable not being written back to DB after evaluation	PCF installed incorrect rules based on PRA status because it did not retain the last known PRA state. PRA status session variables were not written back to the database after evaluation.	2	22.3.2

Table 4-33 (Cont.) Policy 23.2.4 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35781385	Helm bug in cnPCRF 23.2.0 (HPA)	The HPA name for the diameter connector was incorrect and did not match the deployment name, causing the diameter connector pods to not auto-scale.	3	23.2.0
35540092	Intermittent DIAMETER_UNABLE_TO_COMPLY (5012) failures in CCA	PDS encountered a "409 Conflict" response error code when PDS search processing resulted in a "200 OK" response without LDAP data. There was no retry mechanism at PDS, and the error was passed down to the PCRF Core.	3	22.4.5
35731238	Bulk Export Request not exporting all selected configurations	Some screens in CNC Console with common configuration APIs did not support bulk import and export, even though CNC Console had the option to perform data export/import.	3	22.4.2
35775695	[PCF-Audit] Able to enter out of range value for minimum audit attempt field	The range of values that Minimum Audit Attempts field can accept was mentioned as 0-99, while the allowed values is between 0-255.	3	23.2.2

Table 4-33 (Cont.) Policy 23.2.4 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35694960	SM Update is not rejected with 400 BAD REQUEST and cause PENDING TRANSACTIONS	The default behavior of the pending transaction feature was affected when ERROR_CODE_LIST_TO_BYPASS_BULWARK_DEFAULT = "ANY" was configured. On receiving an SM update during an SM update notify from UDR in progress, the SM update should have been rejected with a 400 Bad Request error and tagged as PENDING_TRANSACTIONS by PCF. However, the SM update was accepted even though SM update locking on Bulwark failed.	3	23.2.0
35756404	No RAR/RAA message sent after STR message received from IMS for AF_Signalling	The PCRF Core pod did not respond to the STR messages for AF_SIGNALLING flows when AFDirectReply was set to false.	4	23.2.2
35775898	[PCF-Audit] Wrong format is shown as example for the Minimum Audit Attempts field	In CNC Console, when a user entered a non-numeric value in an integer number field, the error message displayed on the CNC Console was incorrect.	4	23.2.2

Table 4-33 (Cont.) Policy 23.2.4 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35858198	ASA logs have two response codes (5012 and 2001) but there is no 5012 in the metrics	When the PCRF Core pod sent an ASA diameter message, the diameter ASA response contained two response codes: Diameter 5012 DIAMETER_UNABLE_TO_COMPLY and Diameter 2001 DIAMETER_SUCCESS. However, the Prometheus metrics did not include the 5012 response.	4	22.4.5

Note:

Resolved bugs from 23.2.2 have been forward ported to release 23.2.4.

Table 4-34 Policy ATS 23.2.4 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35774082	PCF ATS 23.2.2: TC FAILURES DUE TO DEFAULT DIAMETER IDENTITY	The user is unable to use custom Diameter identity Diameter Gateway after the ATS feature files containing Diameter messages were transitioned from Seagull to DiamSim. This issue arose as the Diameter Identity used within the feature files was set to *oc-diam-gateway* by default and modification of Diameter Gateway's identity resulted in validation failure at DiamSim resulting in Diameter connection failure.	2	23.2.2

Table 4-35 Policy 23.2.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35683052	SmPolicyAssociation DB record corrupted when the configuration Data Compression Scheme changed	There was 500 error on SM create at multiple sites after applying golden configuration.	2	23.1.6
35700060	PDS Stale Session AM Test - AM session NOT deleting even after ForceTTL	AM session was not getting deleted from the database even after MaxTTL+ForceTTL.	2	23.1.7
35700073	PDS Stale Session UE Test - UE session NOT deleting even after ForceTTL	UE session was not getting deleted from the database even after MaxTTL+ForceTTL duration.	2	23.1.7
35727187	AM Stale Session - PolicyDS is NOT deleting database entry when nUDR Connect receives non404 Error for GET Request	For stale PDS data handling for AM service, Policy received a revalidation of N+session after CONCURRENT_REQUEST_GUARD_TIME time flag. Then PolicyDS received non 404 Error response for nUDRconnector GET Request and a nCHF notification with subscriber spendinglimitstatus change with validateuser=True.	2	23.2.2
35691863	Plan Type in UmData is "base" Even though in cnPolicy it is configured as Top-Up	Plan Type in UmData was "base" even though in cnPolicy it is configured as Top-Up.	3	23.2.0
35689677	Update helm hook version for Audit upgrade to 23.2.2 for Audit Service	Due to missing "audit_report" column that was added in 22.1.6 hook, audit might fail.	3	23.2.1
35630450	PCRF-core dont send umPolicyDecision for user provisioned at UDR without umData	The PCRF-core did not send umPolicyDecision to PRE when the user was provisioned at UDR but the umData was not provisioned.	3	23.2.0
35693217	UpdateNotify 503 retry	After the SMF failover, the SM service sent UpdateNotify to the secondary SMF and received a 503 response.	4	23.1.5

Note:

Resolved bugs from 23.2.1 have been forward ported to release 23.2.2.

Table 4-36 Policy ATS 23.2.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35767953	ATS Failure on error logging testcases due to incorrect container selection	In Openshift environment, kubernetes stores istio-proxy as the first container. Therefore, ATS picked up up logs of the istio-proxy container, that is an incorrect selection. This caused the test case to fail.	2	23.2.2
35639240	Verification steps logs of NewFeature are not present in console logs	A verification statement has been added in multiple feature files and it does not generate any logs in the console.	3	23.2.0

Table 4-37 Policy 23.2.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35676108	diam-gw logging enhancement for IP-CAN_SESSION_NOT_AVAILABLE (5065)	When PCF Diameter Gateway was configured with logging level WARN, it did not print any logs while responding with DIAMETER error. For example, IP-CAN_SESSION_NOT_AVAILABLE (3GPP,5065).	3	23.2.0
35584443	Wrong decision in block policy by outdated data	The PRE was making wrong decisions because it did not have updated information.	3	23.2.0
34901684	Policy evaluation on Matchlist is false	Policy evaluation on the matchlist was false.	3	22.3.2
35572327	PDS Work Flow broken after PI-D-22 release (Charging Profile selection based on User Profile)	PDS workflow was broken for charging profile selection based on the user profile. As per 5G call model, UDR data source query should be initiated on the basis of PDS policy. It should not happen by default.	3	22.4.6
35632530	Error Unexpected exception occurred invoking async method	Error Unexpected exception occurred invoking asynchronous method. SUPI was selected as the preferred search index but was not found in the request while running 30K TPS (Call model) traffic with audit enabled.	3	23.1.3
35536055	5GC GETS call failures	PCF returned 5012 error due to 5GC GETS call failures.	4	22.4.0

Note:

Resolved bugs from 23.1.x have been forward ported to release 23.2.1.

Table 4-38 Policy 23.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35369104	Realm based rounting does not work in Diameter Configuration	In CNC Console, while setting Diameter Configurations, the user was unable to add diameter peer node with realm values having underscore (_) as Configuration Management service throws 'invalid domain error'.	2	23.1.2
35330000	PCF traffic drop due to 408 Request Timeout response from NRF	When nrf-client-nfmgmt leader pod switches from primary to secondary pods, the nrf-client-nfmgmt leader pod became unresponsive and stopped sending heartbeats to NRF.	2	22.3.3
35323391	Session Management (SM) receives 403 LATE OVERLAPPING REQUEST	When two different SM Create requests come for different DNNs, the collision detection logic does not resolve it. Instead, the requests were rejected with 403 Error Late Overlapping Request.	2	23.1.1
35293646	On PCF rollback from 23.1.1 to 22.4.4 nrf-client-nfmanagement current version is not updated in ReleaseConfig Table	During PCF rollback from 23.1.1 to 22.4.4, nrf-client-nfmanagement service skipped performing the update to version 22.4.4 in ReleaseConfig database due to missing rollback hook job in its chart.	2	23.1.1
35284478	PCF Audit Configuration for Session Management (SM) and Policy Data Source (PDS) are not saved in database	Audit configuration changes for SM and PDS in CNC Console GUI were not saved to `DB Audit Registration` Table in the database.	2	23.1.1
35210135	PCF traffic drop due to 408 Request Timeout response after Session Management Function (SMF) service crash	The CPU utilization for SM was higher than expected.	2	22.3.3
35073926	Import re-attempt profile feature fails in CNC Console	In CNC Console GUI, import re-attempt profile feature failed to overwrite existing values when run on a system which already had re-attempt profiles configured.	3	22.4.4
35412838	Unable to export Message priority profiles for Sd Application	Configuration Management (CM) Service was unable to export the data for diameter message priority profiles where condition application name is Sd or condition message is Sy-SLR.	3	23.1.4

Table 4-38 (Cont.) Policy 23.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35393724	SM PCF responding with "cause:null" values	JSON schema validation was failed in SMF when error responses, such as 404 Not Found, were sent to SMF with "cause:null" value.	3	22.3.3
35378625	Policy Export fails with certain blockly such as "Set session revalidation time to earliest of"	The Policy Export functionality failed when policy has the blockly "Set session revalidation time to earliest of".	3	23.1.3
35345447	On PCF upgrade, 500 Internal Server Error in Ingress Gateway for SM Policy	PCF upgrade to 22.4.5 resulted in 500 Internal Server Error in Ingress Gateway for SM Policy transactions.	3	22.4.5
35345073	Auth-Application-Answer (AAA) response messages are not recorded	If AAR was sent without Rx-Request-Type AVP to PCRF-core, then the msgType dimension was missing in the occnp_diam_response_local_total metrics .	3	22.4.2
35218840	PDS workflow fails after performing bulk import	PDS workflow did not update after performing bulk import of PDS settings and workflow.	3	23.1.0
35209617	PCF sends Abort-Session-Request (ASR) after successful Session-Termination-Answer (STA) message toward IP Multimedia System (IMS) voice call	After responding with successful STA message to Diameter Gateway, PCF initiated an ASR message towards IMS."	3	22.4.2
35108251	Blockly evaluation for NF type fails	When using NFType blockly for AM and UE, the NFType was not registered by the Policy RunTime Engine (PRE).	3	22.4.4

Note:

Resolved bugs from 22.2.x, 22.3.x, 22.4.x, and 23.1.x have been forward ported to release 23.2.0.

Table 4-39 Policy ATS 23.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35351149	ATS test case "SMF_AltRoute_LocPrefSame_ODD_SVCName" fails	The nf11 stub messages were not cleared from the previously run test casewhich is causing the "SMF_AltRoute_LocPrefSame_ODD_SVCName" test case to fail.	3	23.1.3

4.2.10 SCP Resolved Bugs

Table 4-40 SCP 23.2.3 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35921271	SCP-ATS:OutlierDetectionInterSCP.feature failed due to metrics mismatch	The virtual service with attempt values set to 0 was not applied when using service mesh configuration deployment file.	2	23.2.2
35860234	SCP is rejecting Profile updates for FOREIGN SCP'	SCP marked all the local SCP nfsetids as foreign in local map when the notification pod was reinitialized.	2	22.4.4
35829374	Invalid Api Version in response for notification call-SCP 23.2	API version was invalid in response to notification call-SCP 23.2.	2	23.2.0
35577102	Intermittent DB Operation failure in notification and subscription pod	Intermittent DB Operation failed in Notification and Subscription pods.	2	22.4.4
35857688	Intermittent failures in SCP routing messages from SCP towards various producer NFs	Intermittent failures occured while SCP routed messages toward various producer NFs.	2	23.2.0
35847868	Inter-SCP Routing SCP-P decodes scpPrefix from path incorrectly leaving an extra slash	The consumer SCP (SCP-C) was adding a forward slash at the end of the 3gpp-target-api-root header when sending the service request to producer SCP (SCP-P).	3	23.2.0
35909344	SCP does not have an error log for DNS failures	SCP was missing specific cause and metric for DNS failure.	3	22.3.2
35909394	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 4-41 SCP ATS 23.2.3 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35860302	SCP ATS: Database tables cleanup issue post failure of a feature	The database tables were not properly cleaned up and reverted to their default values. Therefore, there were stale entries in the database.	2	23.2.2
35860272	SCP ATS: SCP_22.3.0_Bug_Fixes feature is failing in regression run	The SCP_22.3.0_Bug_Fixes feature was failing in the regression run due to metric mismatch.	2	23.2.2
35860160	SCP ATS 22.4.2/SCP 22.4.4 New Features - S23 static config test case failed under SCP_Lci_Support.feature	The LCI header validity date was a fixed value, not modifiable.	3	22.4.2

Note:

Resolved bugs from 22.4.3 and 23.1.3 have been forward ported to Release 23.2.3.

Table 4-42 SCP 23.2.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36070406	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
35736480	Content Type being changed by SCP to PCF	Content Type was changed by SCP from application/json to application/problem+json.	2	22.3.2
35769243	Notification pods have been continuously crashed after the upgrade from 23.2.1 to 23.2.2	Notification pods crashed continuously after upgrading from 23.2.1 to 23.2.2.	2	23.2.2
35679353	SCP-ATS:SCP_HealthCheck_Support_P0.feature getting failed when we upgrade SCP from 22.4.2	SCP_HealthCheck_Support_P0.feature failed while upgrading SCP from 22.4.2 to 23.2.1.	2	23.2.1
35697475	SCP-ATS 23.2.1: S1 of GlobalEgressRateLimiting feature is failing in regression run	The GlobalEgressRateLimiting feature failed in the regression run.	2	23.2.1
35680394	SCP not clearing all alarms in case of change of threshold to higher value for Pod Overload Feature	For the Pod Overload Control feature, SCP did not clear all the alarms when the threshold value was changed to a higher value.	3	23.2.1

Table 4-42 (Cont.) SCP 23.2.2 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 the traffic at 231K TPS using 8vCPU and 12vCPU worker pod profiles.	3	23.1.0

> **Note:**
>
> Resolved bugs from 22.4.3 and 23.1.3 have been forward ported to Release 23.2.2.

Table 4-43 SCP 23.2.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35584563	SCP fails to establish Kafka connection after In-service rollback was performed	SCP failed to establish Kafka connection after in-service rollback was performed.	2	23.2.0
35579770	Transaction drop observed while running the traffic at the rate of 231K TPS on SCP 23.2.0	Transaction drop was observed while running the traffic at the rate of 231K TPS on SCP 23.2.0.	2	23.2.0
35608768	SCP:- AMF - NudmUECM_Amf3GPPAccessInfoUpdate - 400 Bad Request	The location header was incorrectly updated with producer SCP alias resulting in routing failure for subsequent requests.	2	22.3.2
35308635	Worker and load manager pods restarted while running traffic at 230K TPS with the LCI and Ingress rate limit features enabled	SCP-Worker and SCP-Load manager pods restarted while running traffic at 230K TPS with the Load Control Information (LCI) and ingress rate limit features enabled.	2	23.2.1
35441328	SCP 23.1.1 Changes snssais format in the delegated discovery request from SCP to NRF	SCP was updating snssais format while sending delegated discovery request to NRF.	3	23.1.1
35502318	Correction is required in the default SCP deployment to update the fqdn of nnrf-auth2 according to the NRF profile registered	Correction was required in the default SCP deployment to update the FQDN of nnrf-auth2 according to the registered NRF profile.	3	23.2.0
35550506	SCP 23.2.0 install failing with nrfProxyOauthService deployed with debug-tools	Helm charts for nrfProxyOauthService were missing volume details required for debug-tools.	3	23.2.0
35495203	DBTier upgrade from 23.1.1 to 23.2.0 is failing due to mismatch of parameter	cnDBTier upgrade from 23.1.1 to 23.2.0 failed becasue the charts did not match the parameters in the SCP 23.2.0 custom values file.	3	23.2.0

Table 4-43 (Cont.) SCP 23.2.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35579079	SCP 23.2.0 500_INTERNAL_SERVER_ERROR in SCP pod logs post upgrade to PI-B	The enabling of otelTracingEnabled resulted in exception in SCP-Worker.	3	23.2.0
35656949	Intermittent Failures observed in Worker Pod Overload Config API	Intermittent failures were observed in the SCP-Worker Pod Overload Config API.	3	23.2.0
35590657	SCP ATS 23.2.0: Pod overload ctrl default config is not setting back during cleanup	Default range for abatement time was not getting updated during upgrade to SCP 23.2.0.	2	23.2.0
35621597	SCP ATS 23.2.0: S80 of ModelD_based_Routing feature is failing	The intermittent race condition in NRF- Proxy resulted in incorrect status code for routing failures.	3	23.2.0

Table 4-44 SCP ATS 23.2.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35417574	23.1.0_Bug_Fixes.feature:174 Scenario-3 failed with "Actual Count For All Services : -1 Expected Total Count: 0	The validation of ocscp_worker_outstanding_requests was causing the failures. The ATS feature file was corrected to resolve the issue.	3	23.1.2
35543855	SCP ATS 23.2.0: Oracle Internal LAB: SCP_Lci_Support_Miscellaneous feature is failing	The feature file conflict with another concurrent group was causing a stale NF profile thereby resulting in failure.	3	23.2.0
35590802	SCP ATS 23.2.0: Spelling error in Notification_Correlation_Header_model_C feature	In SCP-ATS 23.2.0, there was a spelling error in the Notification_Correlation_Header_model_C feature.	3	23.2.0
35578186	SCP ATS 23.2.0: Oracle Internal LAB: DefaultNotificationCallbackUriModelC_p1 feature is failing	A conflict with another feature file in the concurrent group resulted in update of Model D feature configuration and led to failure.	4	23.2.0

Note:

Resolved bugs from 22.4.3 and 23.1.3 have been forward ported to Release 23.2.1.

Table 4-45 SCP 23.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35317027	Registered With APIversion 1.1.0.0 NF Discovery via SCP is failing with Profile Validation Failed	APIversion 1.1.0.0 in the NF profile validation was failing at SCP during NF discovery.	2	23.1.0
35308635	Worker and load manager pods restarted while running traffic at 230K TPS with the LCI and Ingress rate limit features enabled	The SCP worker and load manager services were not performing as expected while running traffic at 230K TPS with the LCI feature enabled.	2	23.1.0
35495203	DBTier upgrade from 23.1.1 to 23.2.0 is failing due to mismatch of parameter	The default DBtier file provided with the SCP custom template had some missing parameters as per the General Availability (GA) and resulted in failure.	3	23.2.0
35396786	Host header to be removed before sending request to Mediation	For routing, the Istio sidecar adds the host header to :authority. As a result, the presence of the header in the request was causing a problem. When using the Istio sidecar container, the host header was expected to be removed before the scp-worker sent a request to the mediation microservice.	3	23.1.0
35226412	SCP Multiple documentation issues reported	The details of the SCP-Mediation Service parameters were not documented in the SCP Guide. Some hyperlinks were broken in the User Guide.	3	22.4.0
35281252	Helm Warnings observed during Helm upgrade, 'duplicate name "podStatusRetryCount"'	During SCP upgrade, a Helm warning 'duplicate name "podStatusRetryCount" was observed.'	3	22.2.4
35264179	ocscp_metric_remote_response_without_server_header_total Metrics is not pegged when SCP should return an error with a server header that includes its own FQDN and send it to the consumer in case error response received without server header	The ocscp_metric_remote_response_without_server_header_total metric was not pegged when SCP returned an error with a server header that included its own FQDN and sent it to the consumer in case an error response was received without a server header from the primary and secondary producers and the tertiary producers timed out.	3	23.1.0

Table 4-45 (Cont.) SCP 23.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35228349	SCP is not performed alternate routing as per details present in location header in case of response with error "308 Permanent redirect" is receieved from producer and matched with rerouteConditionList in routing options.	SCP wasn't performing alternate routing in accordance with the details present in the location header even when a response from the producer with the error "308 Permanent redirect" was received and matched with `rerouteConditionList` in the routing options.	3	23.1.0
35227720	SCP is not performed alternate routing in case of response with error "429 Too Many Request" is received from producer and matched with rerouteConditionList in routing options.	SCP wasn't performing alternate routing when a response with the error "429 Too Many Requests" was received from the producer and matched with `rerouteConditionList` in routing options.	3	23.1.0
35163108	SCP Upgrade Fails (SCP-Config Pre Upgrade)	Preupgrading of configuration pods failed because SCP was unable to add the new column NF_Instance_Id to the INGRESS_RATE_LIMITER database.	3	22.1.4
35128504	SCP not populating "message-direction" metadata as per requirement	SCP wasn't populating "message-direction" metadata according to the requirement, and was instead using different names.	3	22.4.0
35081076	SCP not showing the load for Inter-SCP and SEPP in load metrics	SCP was not showing the load configured for inter-scp and sepp in the ocscp_nf_load and ocscp_scp_load metrics.	3	23.1.0
35063299	SCP and NF Load metrics were nonfunctional for LCI feature	SCP and NF load metrics weren't functioning properly for the Load Control Information feature.	3	23.1.0
35058870	SCP returns error while configuring SBI Message Priority with httpMethods	SCP was returning an error while configuring SBI Message Priority with httpMethods.	3	22.4.1
35033180	SCP-Mediation-test Microservice Defined in User Guide But Not yaml, Elsewhere	Mediation test service resources were missing in SCP deployment file.	3	22.4.0
34968688	5G SCP: NRF is not present in nfprofile	NRF profile on SCP was deleted because NF profiles had been accidentally registered there with the same NF instance ID as NRF.	3	22.3.0

Table 4-45 (Cont.) SCP 23.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34844014	Observed worker pod restart when network latency is high more than 1 sec.	Due to the large number of requests pending to be processed, it was seen that the worker pod restarted when network latency was higher than one second.	3	22.4.0
35255870	Incomplete information about Egress Host Preference parameters provided in the User Guide that differs from actual implementation	Information on response and FQDN resolution parameters for configuring Egress Host Preference was not documented in User Guide.	3	23.1.0
35302721	"SCP CPU usage Percentage" and "SCP Memory usage Percentage" metrics queries are not working in the latest SCP Dashboard with CNE.	Some metrics are not supported in the latest Prometheus CNE leading to failure of "SCP CPU usage Percentage" and "SCP Memory usage Percentage" charts on the SCP Metric Dashboard.	4	23.1.0
35302303	Namespace is missing from the SCP dashboard metrics queries	Some queries were missing namespace on the SCP Metric Dashboard.	4	23.1.0
35301673	SCP GUI is giving unidentified error if Global Egress Rate Limit parameters are not provided	SCP GUI was displaying unidentified errors when Global Egress Rate Limit parameters were not provided.	4	23.1.0
35283578	SCP console GUI is not having defaultNotificationSubscriptions under NF Profile Rule Configuration	SCP CNC Console GUI was missing defaultNotificationSubscriptions in the NF Profile Rule Configuration section.	4	23.1.0
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, the SCP CNC Console GUI was displaying an unidentified error.	4	23.1.0
35279019	SCP GUI is giving unidentified error if ModeId Routing parameters are not provided	SCP GUI was displaying an unidentified error when ModeId Routing parameters were not provided.	4	23.1.0
35278439	SCP shows inconsistency for the ocscp_nf_service_type parameter value in http_req_host_type_total metrics when sending notification messages.	SCP displayed inconsistency for the ocscp_nf_service_type parameter value in the http_req_host_type_total metrics when sending notification messages.	4	23.1.0
35341901	Alerts file needs to be updated in relation to the 8vCPU and 12GB memory profile for metrics that contain the maximum mps supported by SCP	The alerts file must be updated in relation to the 8vCPU and 12GB memory profile for metrics that contain the maximum MPS supported by SCP.	4	23.1.0

Table 4-45 (Cont.) SCP 23.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35255824	SCP returns 500 Internal error when a mandatory parameter is missing while configuring egress host preference	SCP returns 500 internal error when a mandatory parameter is missing while configuring egress host preference.	4	23.1.0
35173746	Incorrect Cause value "validation on Reroute condition failed" is coming in status code "400" while configuring the unsupported msg format in Reroutecondition list of routing option.	The incorrect cause value "validation on Reroute condition failed" is returned in the status code "400" when the invalid message format is configured in the reroutecondition list of routing options.	4	23.1.0
35066507	SCP changes the scheme to http while producer is sending the notification message with Callback and api-root header on TLS enabled set up	While the producer was sending the notification message with a callback and an api-root header on a TLS enabled setup, SCP was changing the scheme to http.	4	23.1.0
35032731	Warnings about duplicate names appeared when upgrading SCP	When SCP was upgraded, warnings related to duplicate names appeared.	4	22.4.1
35004850	SCP returns 500 internal error in case of sending the GET request for NF profile based on service name	When the GET request for the NF profile based on the service name was sent, SCP returned a 500 internal error.	4	22.4.0
34999205	Correlation id, consumer fqdn & consumer id is missing sometimes in metadata list	Consumer ID, consumer FQDN, and correlation ID were occasionally missing from the metadata list.	4	22.4.0
34945609	SCP responded with an incorrect error cause when out-of-range values were provided for the Outlier Detection configuration parameters	When out-of-range values were provided for the Outlier Detection configuration parameters, SCP responded with an incorrect error cause.	4	22.4.0
34235083	SCP responded with incorrect problem details in https response body in case of Producer NF not available	When producer NF was unavailable, SCP responded with incorrect problem details in the https response body.	4	22.2.0
34093830	SCP not responding with the correct cause in case of missing discovery headers in Implicit Notification Request	SCP was not responding with the correct cause when the discovery headers in the implicit notification request were missing.	4	22.1.1
35349229	Unable to create template yaml file with commands on SCP installation guide || Configuration values.yaml file name is mentioned wrongly in the scp installation guide	In the SCP Installation Guide, the ocscp-values-23.1.0.yaml file name was incorrectly written as ocscp-custom-values-23.1.0.yaml file.	4	23.1.0

Table 4-45 (Cont.) SCP 23.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35349020	helm repo update is giving an unexpected error if we follow SCP Installation guide || The namespace and values.yaml file name is mentioned wrongly in the scp installation guide	In the SCP Installation Guide, the ocscp-values-23.1.0.yaml file name was incorrectly written as ocscp-custom-values-23.1.0.yaml file, and there was no instruction to install Helm.	4	23.1.0
35274368	Documentation should be updated to reflect that no action is taken by SCP when an absolute URL is received in location from the producer while the Egress Host Preference feature is enabled	In the SCP REST API Guide, there was no mention of tasks to be performed by SCP when an absolute URL was received in the location header from the producer NF while the Egress Host Preference feature was enabled.	4	23.1.0
35145653	Missing description of exceptionErrorResponses	In the SCP REST API Guide, there was no description about exceptionErrorResponses in the Routing Options section.	4	22.4.0
35133806	Description for Outlier detection needs improvement	In the SCP User Guide and REST API Guide, the description for Outlier Detection feature did not clarify the definition of error codes received by SCP.	4	22.4.0

Table 4-46 SCP ATS 23.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35298113	OutlierDetectionProducer_AUSF.feature getting failed on full regression run	Issues with validation in test cases resulted in an ATS failure.	2	23.1.1
35306715	SCP ATS regression NRF_Subscription Scenarios failed	Multiple subscription threads were created causing duplicate subscriptions and ATS failure.	3	22.4.2
35374727	SCP_Mediation_Cases Fails Step "Then update mediation configmap set" in .../nf_rules_for_all_scenarios.drl	ATS was failing due to a hyphen in the deployment name in the configuration map.	3	22.3.0
35187576	SCP_Observability_And_Inter_Microservice_Resilience feature is failing	The ATS was failing because pod scaling was taking longer than the maximum wait time.	3	23.1.0
35396733	SCP ATS unable to deploy PCAP Log Collection Feature	The default service account was missing required permission that caused PCAP log collection failure.	4	23.1.0

> **Note:**
>
> Resolved bugs from 22.2.4, 22.4.3, 23.1.1, and 23.1.2 have been forward ported to Release 23.2.0.

4.2.11 SEPP Resolved Bugs

SEPP 23.2.2 Release

There are no new resolved bugs in this relrease.

> **Note:**
>
> Resolved bugs from 23.1.x and 23.2.x have been forward ported to Release 23.2.2.

Table 4-47 SEPP 23.2.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35478340	Get 400 and 500 Error codes from EGW when requests are routed to multiple SEPPs.	When the traffic was sent from consumer SEPP to one Producer Remote SEPP, traffic flow was as expected. But, as soon as the traffic was sent to more than one Producer Remote SEPPs, the Gateway displayed the error and the traffic could not be sent beyond 70 TPS.	2	22.3.2
35375298	SEPP reports the Error 500 "No Matching Route."	There was a race condition causing the route deletion at the Gateway. Hence, SEPP was not able to download the correct route for routing.	2	23.2.0
35444002	Unexpected drop observed in Ingress and Egress while running 9K message copy traffic.	Unexpected drop was observed in Ingress and Egress while running 9K message copy traffic with the error "Circuit Breaker moving into open state".	2	23.2.0

Table 4-47 (Cont.) SEPP 23.2.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35649651	SEPP TLS Handshake incorrectly reestablishes after Remote SEPP Set is deleted and Remote SEPP01 is disabled in SEPP02.	Issue 1: Without changing `isEnabled=TRUE`, handshake was created again successfully, and the peer was created in in common configuration table. Issue 2: RemoteSepp could not be deleted when`isEnabled` was set to False.	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 were restarting during the cnDBTier rollback to 23.2.0.	3	23.1.0
35659123	podname blank in SEPPPodMemoryUsageAlert and SEPPPodCpuUsageAlert .	podname was blank in `SEPPPodMemoryUsageAlert` and `SEPPPodCpuUsageAlert`. `alertname=SEPPPodCpuUsageAlert appname=pn32f-svc container=pn32f-svc namespace=gg-sepp2 oid=1.3.6.1.4.1.323.5.3.46.1.2.4002 podname= severity=warning`	4	23.2.0

Note:

Resolved bugs from 23.1.x and 23.2.0 have been forward ported to Release 23.2.1.

Table 4-48 SEPP 23.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35335979	Call failure observed with error code 503, 504, 408, and 500 during the performance run at 62K MPS on SEPP_23.1.1 Setup.	The call failure was observed with the error codes 503 ,504 ,408, and 500 during the performance run at 62K MPS on SEPP_23.1.1 Setup. This issue is fixed as a part of performance enhancement.	2	23.1.1
35331585	Call failure observed after Topology Hiding applied at 3gpp-sbi-target-apiroot header's during performance run.	The call failure was observed after the Topology Hiding feature was applied at the headers during the performance run at 62K MPS at SEPP_23.1.1_Model-B setup.	2	23.1.1
35415179	Scheme in 3gpp-sbi-target-apiroot header changes from https to http	The scheme in 3gpp-sbi-target-apiroot header was changed from https to http while sending traffic from C-SEPP to P-SEPP or P-SEPP to C-SEPP.	2	23.1.1
35307166	When SEPP deployed with ASM is enabled, SEPP metrics are not being displayed on prometheus.	These metrics were not displayed because of the scraping of the port set for cn32f, pn32f, and config-mgr. Port set was 9090, but data could be fetched on port 9092.	2	23.1.1
35367896	SOR: Dynamic update to SoR trigger list not taking effect in case the API is removed	After removing the API from SoR trigger list and waiting for more than five minutes, the traffic was still being routed to SoR. The internal cache was created to store the SoR trigger list was not getting cleared when the entries were deleted. The code list was updated to clear the cache.	2	23.1.0
35273688	Network Id validation checking the last element of array guamiList	Cat-2 Network Id Validation on body validates the plmn id in the guamiList. If the guamiList has multiple plmn Ids, only the last element of the array is considered for validation. If any plmn id before the last element is invalid, then the request passes through SEPP successfully. Now all the plmnIds in the guamiList arrays are validated.	3	23.1.0

Table 4-48 (Cont.) SEPP 23.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35337221	SEPP ATS installation failed on Tanzu Cluster.	The SEPP ATS installation failed at Tanzu Cluster. While doing the SEPP ATS installation running the following command, , helm install ocats ocats-sepp-23.1.2.tgz -f ocats_oC-SEPP_values_23.1.2_ys-sepp_v1.yaml -n ys-sepp The following error occurs: "unable to build kubernetes objects from release manifest: [unable to recognize “”: no matches for kind “ServiceEntry” in version “networking.istio.io/v1alpha3”, unable to recognize “”: no matches for kind “VirtualService” in version “networking.istio.io/v1alpha3”]" Some extra labels were present in the deployment. To remove that, serviceEntry.yaml and virtualService.yaml were deleted from the template, then the deployment was successful.	3	23.1.1
35219763	SEPP 22.3.x prometheus alert rules for CPU or memory usage need to match default config allocations and be limited to SEPP pods	The "SEPPPodCpuUsageAlert" and "SEPPPodMemoryUsageAlert" triggered incorrectly as the alerts were miscalculated. The default yaml file allocates more memory and CPU to different SEPP microservices. This miscalculation is causing the alerts to trigger incorrectly.	3	23.1.0
35211643	SEPP pods deployment configurations must be edited for OSO integration after SEPP fresh installion and upgrade.	After following the steps for SEPP integration with OSO during SEPP installation and upgrade, the deployment configurations of SEPP pods must be edited. It causes SEPP pods to restart. Some of the common services charts are not updated to handle the connection with OSO.	3	23.1.0
35083520	Clearance issue for alert SEPPN32fTopologyBodyOperationFailureAlert	Some alerts were not cleared after the performance traffic stopped for SEPPN32fTopologyBodyOperationFailureAlert and SEPPPodMemoryUsageAlert. The expressions are updated.	3	22.4.0

Table 4-48 (Cont.) SEPP 23.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34724440	Request Failures observed at the beginning of performance run	The user observed a few failures while the performance run was initiating. Hence, updated the default value of REQUEST_TIMEOUT and CONNECTION_TIMEOUT in custom_values.yaml file. This is due to the REQUEST_TIMEOUT happening at plmn-ingress-gateway and n32-egress-gateway, when the network is slow and not able to send the response in designated time. The first few queries take more time on gateway as they perform DNS resolution. Note: User has to set the REQUEST_TIMEOUT and IDLE_TIMEOUT values in custom_vaues.yaml considering the network latency and delays.	3	22.3.0
34664359	SEPP microservices traces are not correlated in Jaeger UI	In previous versions, when querying traces on JAEGER UI, one single trace was returned with multiple spans from the different microservices involved for a single transaction. For example: plmn-ingress-gateway span + cn32f span + n32-egress-gateway span. In 22.3.0, this correlation is corrected and every microservice is generating a different trace. The fix is provided by API Gateway.	3	22.3.0
35014266	"Server" header not present when the requests are rejected by SEPP due to rate limiting	Ingress rate limiting is configured at hosted SEPP. When the traffic is beyond the configured limit, the requests are rejected as configured, but server header is absent. Body: {"type":null,"title":null,"status":429,"detail":"TOO_MANY_REQUESTS","instance":null,"cause":null,"invalidParams":null} Solution: Added the 429 in the list of ErrorCodesSeriesList in plmn-ingress-gateway errorCodeSeriesList: - id: E1 errorCodeSeries: # Possible values for "errorSet" attribute: 5xx, 4xx, 3xx, 2xx, 1xx - errorSet: 4xx errorCodes: - 400 - 408 - 404 - 429	3	22.4.0

Table 4-48 (Cont.) SEPP 23.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35379697	Install fails when Debug tools and Mediation are enabled together	SEPP installation failed when mediation and debug tools were enabled together. If any of the two was disabled, installation was successful.	3	23.1.0
35407842	Partner SEPP rejects the n32 handshake due to Oracle SEPP including the advisorCount parameter in JSON payload	Oracle SEPP attempts a handshake to partner non Oracle SEPP that was just upgraded and partner SEPP rejects the handshake with the 400 Bad Request Error. This is due to the Oracle SEPP sending the handshake with parameter advisorCount: 1 in TLS handshake message. Extra field is added during the POJO to JSON conversion while creating the handshake request and response.	3	22.4.0
35292187	Correct the metric names of following metrics: ocsepp_network_id_validation_body_failure_total and ocsepp_network_id_validation_header_failure_total	Updated the names of the following metrics in the metrics section in the SEPP User Guide: ocsepp_network_id_validation_body_failure is updated to ocsepp_network_id_validation_body_failure_total ocsepp_network_id_validation_header_failure is updated to ocsepp_network_id_validation_header_failure_total	4	23.1.0
35357612	SEPP User guide update required for SoR Metrics dimensions	The following metrics are updated and missing dimensions are added: ocsepp_pn32f_sor_requests_total ocsepp_pn32f_sor_responses_total ocsepp_pn32f_sor_failure_total The following updates are done on dimensions: The plmnid is not required in the listed metrics, hence remove the plmnid. The dimension, domain is not present in the listed metrics, instead peer_domain is present, hence pdated the peer_domain. The dimension RoamingPartnerName is updated to remote_sepp_name.	4	23.1.1
35221582	Response status code needs to be updated for API used to add a specific rule to an existing list	In the following API, response code "201 Created" is documented instead of "200 Created": /sepp-configuration/v1/security-counter-measure/network-id-validation-allowed-list/update-rules/{networkIdValidationListName}	4	23.1.0

Table 4-48 (Cont.) SEPP 23.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35109079	SEPP Alert is showing BSF pods detail in pod	While testing the alerts for SEPP, the SEPPPodMemoryUsageAlert was showing the details of BSF namespace. The details of BSF namespace as incorrect alert expression was used.	4	23.1.0
35098773	SEPP 22.3.1 Request for Documentation Improvement	The users requested for improvement in documentation of Installation, REST API, and User guides.	4	22.3.1
35053377	CNC Console GUI does not provide option to change mediation service log level	At present, the mediation service is not listed on CNC Console GUI. Hence, its log level can't be changed using CNC Console.	4	22.4.0
34920721	SEPP sending "5g-sbi-message" with a New line and Tabs (\n & \t) on Kafka	5G SBI message sent at Kafka (for both call flows and Erroneous Scenarios) when Message copy is enabled on all Gateways is sent along with special characters like new line and Tabs "\", "\n", "\t" so on along with the "5g-sbi-message.	4	22.4.0

Note:

Resolved bugs from 23.1.x have been forward ported to Release 23.2.0.

4.2.12 UDR Resolved Bugs

UDR 23.2.2 Resolved Bugs

There are no new resolved bugs in this release.

Table 4-49 UDR 23.2.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35795813	IGW svc_pending_count increasing updates without decrementing	Overload was triggered in Ingress Gateway for PCF-SM.	2	23.1.6
35299116	Pending Message count metric is showing 10x higher values compared to IGW 23.3.4	While performing NRF benchmarking with Ingress Gateway 23.3.5, the pending message count reported at Ingress Gateway was 10 times higher. Each pod displayed a pending message count of around 1500.	2	23.3.5

> **Note:**
>
> The above resolved bugs are back ported from ingress gateway 23.4.x release.

Table 4-50 UDR 23.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35348719	Problem Statement : PATCH request for sm-data is failing if AM-DATA is provisioned under POLICY_DATA (when AE is enabled)	When auto enrollment was enabled and AM-DATA was provisioned under POLICY_DATA, the PATCH request for sm-data failed.	2	23.1.0
35299116	PUT Operation on UsageMon Data is not creating default SmPolicySnssai Data	PUT Operation on UsageMon Data failed to create default SmPolicySnssai Data even if the auto enrolment was enabled.	2	23.1.0
35374915	idleTimeout has incorrect value in CV-Document to be updated	nudr-drservice.hikari.idleTimeout value was updated from 420000 to 420 in the UDR installation guide.	2	22.4.1
35152038	Subscribers not migrated when there is a large separation between subs/msisdns numbers	The subscribers were not migrated to the database when the range between subscribers and Mobile Station Integrated Services Digital Network (MSISDN) numbers was more.	2	22.4.0
35409689	PROVGW- In Provgw service configuration Retry error codes are not editable through CNCC for SLF and UDR mode	In the Provision Gateway service, the configuration retry error codes were not editable through CNC Console for SLF and UDR modes.	3	23.1.1
35356211	Bulk Migration - Schema validation failed.	Schema validation was failing for bulk import migration.	3	23.1.1
35353343	GET request is returning 404 not found even after PUT is successful with 404 (With AE Enabled)	GET request was returning 404 not found error with auto enrollment enabled but the PUT operation was successful.	3	23.1.0
35337002	No Validation for limitId in UmData , Null string is also accepted in PUT Request	Null string was accepted in the PUT request, and there was no validation for limitId in UmData.	3	23.1.0

Table 4-50 (Cont.) UDR 23.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35327742	SNSSAI: & DNN fields are not editable from CNCConsole for Auto-Enrollment feature	Single - Network Slice Selection Assistance Information (S-NSSSAI) and Data Network Name (DNN) fields were not editable from CNC Console for auto enrolment feature.	3	23.2.0
35264074	PATCH is rejected with reason 400 schema validation failed even after enabling Auto-Enrolment	After enabling auto enrollment feature, the PATCH operation was rejected with reason 400 schema validation failed.	3	23.1.0
35251872	Change the External Traffci Policy on the diam-gateway of the cnUDR	externalTrafficPolicy flag was added in the custom-values.yaml.	3	22.4.0
35238832	Provisioning of State to VSA in SM-DATA is not increasing ETAG Value	Entity Tag (ETAG) value was not incrementing after provisioning of State to Vendor Specific Attributes (VSA) in SM-DATA.	3	23.1.0
35227673	Subscriber Activity logging issues in UDR	Response for POST and Delete method was not logged in subscriber activity logging in UDR.	3	23.1.0
35144401	Subscriber Data Not exported with multivalue delimeter	Configuration with multiple value field delimiter was successful but the subscriber data was not exported.	3	23.1.0
35143779	Problem Statement: EIR Data not exported properly for MSISDN	Equipment Identity Register (EIR) data was exported incorrectly for Mobile Station Integrated Services Digital Network (MSISDN).	3	23.1.0
35138364	StartTime Validation Failing	PUT curl command was not validating the daily start time and weekly start time.	3	23.1.0
35138165	Failure metrics are not getting pegged for Bulk import on Login Denied	The failure metrics were not getting pegged when login was denied for the bulk import tool.	3	23.1.0

Table 4-50 (Cont.) UDR 23.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35129182	Export tool Is not exporting EIR data as per the IMSICOUNT/ MSISDN COUNT	The export tool was not exporting EIR data as per the International Mobile Subscriber Identity (IMSI) count and Mobile Station Integrated Services Digital Network (MSISDN) Count.	3	22.4.0
35102511	EIR Solution is not printing size of import/ export file in logs	EIR solution was not printing the size of import and export file in logs indicating the file transfer from remote server.	3	22.4.0
35065841	PUT operation for BULKIMPORT accepts invalid values	The bulk import PUT operation was accepting invalid values.	3	22.4.0
35041066	Discrepency in UDR 22.4.1 installation yaml file	There was discrepancy in UDR 22.4.1 installation yaml file in percentage based PDB configuration.	3	22.4.1
34940342	EIR PDBI DLT_EIR is not deleting the KEY from EIR DATA if executed immediately after Update	If upd_eir or dlt_eir was run before ent_eir, the upd_eir or dlt_eir would fail.	3	22.4.0
34756798	UDR security vulnerability: readOnlyRootFilesystem Set to False	The readOnlyRootFilesystem in the yaml file was set to False. This controls whether a container is able to write into the root file system.	3	22.3.0
35247269	Migration_Tool in cnUDR doesn't work	Migration tool was not starting because the 4G UDR connection was not correct.	3	23.1.0

Note:

Resolved bugs from 23.1.x and 22.4.x have been forward ported to Release 23.2.0.

4.2.13 Common Services Resolved Bugs

4.2.13.1 Egress Gateway Resolved Bugs

Release 23.2.4

Table 4-51 Egress Gateway 23.2.4 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release	Fixed in Release
35391273	SCP Monitoring egw api is not returning the correct status of configured peer	Egress Gateway didn't return the correct status of the configured peers when they were configured with health API and peermonitoring was enabled.	2	23.2.2	23.2.4
35391415	[SCP Monitoring] oc_egressgateway_peer_health_status is not getting pegged correctly	The oc_egressgateway_peer_health_status metric was not pegged correctly in Egress Gateway.	2	23.2.2	23.2.4
35380234	oc_egressgateway_peer_health_status metric provides value as 1 even after the peer configuration is removed	oc_egressgateway_peer_health_status metric returned value 1 even after a peer was removed from peer configuration. The oc_egressgateway_peer_health_status metric is used for performing health checks on all configured SCP peers. The SCP_PEER_UNAVAILABLE alert was defined on this metric to raise an alert whenever it's value does not equal 0. When the customer decided to remove one of the SCP peers entirely from configuration because the SCP peer was unhealthy or a new SCP peer was configured to replace it, this metric still showed up with the peer name in Egress Gateway with a value of 1. As a result, the alerts never never got resolved.	2	23.2.1	23.2.3

Table 4-51 (Cont.) Egress Gateway 23.2.4 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release	Fixed in Release
35381653	No Configurable option for 'maxUnavailable' & 'maxSurge' during Rolling Upgrade	NSSF needed to upgrade NSSF and Egress Gateway pods one at a time because they were facing significant traffic drop during upgrade and rollback as compared to other NFs. They needed to set maxSurge: 1 and maxUnavailable: 0 and these parameters should be exposed in the Egress Gateway values.yaml file.	2	23.1.0	23.2.3
35336043	EGW not able to fetch config-map details saying - "config-map with name : <config-map-name> not present in namespace : <ns> "	Multiple services had observed the "config-map with name : <config-map-name> not present in namespace : <ns>" error when they attempted to read from config-map of Egress Gateway.	2	22.4.4	23.2.3
34710690	microservices traces are not correlated in Jaeger UI	When traces are queried on JAEGER UI, one single trace should be returned with multiple spans from the different microservices involved in a single transaction. This correlation was not happening and every microservice was generating a different trace.	2	22.3.4	23.2.3
35258741	Policy ATS regression scenario UDR_SessRetry_UseAlternateSCP_Enabled failing	The Policy ATS regression scenario UDR_SessRetry_UseAlternateSCP_Enabled was failing because the reroute to alternate SCP failed and the request was rerouted to nf21 with udr 3.	2	23.2.0	23.2.1

Table 4-51 (Cont.) Egress Gateway 23.2.4 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release	Fixed in Release
35352640	Egress GW 23.2.1 - Duplicate headers added in 401 error response returned to connector services of PCF after retries attempted at egress gateway	The duplicate headers added in 401 error response were returned to the PCF connector services after retries were attempted at Egress Gateway.	3	23.2.1	23.2.3
35322756	oc_egressgateway_peer_health_status metric not showing up when pod comes up	Egress Gateway peer health check metric oc_egressgateway_peer_health_status didn't get generated unless a peer was down. It became available after the peer was made unavailable.	3	23.2.1	23.2.3
34838890	No Configurable option for 'maxUnavailable' during Rolling Upgrade	Gateway Common Service charts didn't have the option to configure the maxUnavailable percentage during upgrade.	3	22.4.0	23.2.3
35322756	oc_egressgateway_peer_health_status metric not showing up when pod comes up	Egress Gateway peer health check metric oc_egressgateway_peer_health_status didn't get generated unless a peer was down. It became available after the peer was made unavailable.	3	23.2.1	23.2.2
35232037	EGW Pod Logs doesn't contain SNI Feature statement for ASM "Service mesh is enabled. As a result, SNI will not be populated even though it is enabled"	After the TLS connection is successfully established in ASM setup, the client hello message was sent without SNI header. However, the debug log statement "Service mesh is enabled. As a result, SNI will not be populated even though it is enabled" was missing.	3	23.2.0	23.2.2
35097588	IGW and EGW are not sending uber-traced-id in header.	Egress Gateway was neither able to send the uber-traced-id in the header nor able to create the uber-trace-id when a request didn't have a header.	3	23.1.0	23.2.2

Table 4-51 (Cont.) Egress Gateway 23.2.4 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release	Fixed in Release
34610824	Message copy- Data sent to Kafka does not contain multiple via header values	The message copy data that was sent to Kafka didn't contain multiple via header values.	3	22.3.0	23.2.2
35014846	Observing Cancellation Exception in IGW and 503 Service unavailable on EGW of 23.1.0 images which corresponds to 23.1.0 release.	"503 Service Unavailable" error was observed in Ingress Gateway release 23.1.0.	3	23.1.0	23.2.0
35178640	Getting warning during helm install for ingress, egress and alternate route services	The customer was getting a warning on CNE version 22.3.0-rc.2 and Kubernetes version v1.23.7 when they performed a Helm install for Egress Gateway.	3	23.1.0	23.2.0
34708261	adding x-request-id in the IGW/EGW logs for easy co-relation with sidecar container log	Gateway Services provided ocLogId for correlation between the logs generated between NF microservices. However, the container required to correlate between the Sidecar message and the application was missing. As a temporary work around, NF used timestamps, however that wasn't sustainable during performance load. As a resolution, the container was provided. Sidecar container raised x-request-id and added it to a header for tracing the message across multiple pods. This header value was added in log messages as an attribute for debugging.	4	22.3.0	23.2.0

Table 4-51 (Cont.) Egress Gateway 23.2.4 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release	Fixed in Release
34930585	Gateway sending "5g-sbi-message" with a New line and Tabs (\n & \t) on Kafka	The 5g-sbi-message sent at Kafka(for both call flows and Erroneous Scenarios) when Message copy was enabled on all Gateways was sent along with special characters such as new line and tabs "\", "\n", "\t" etc along with the "5g-sbi-message".	4	22.4.1	23.2.0
35069040	PLMN egw server headers in response is repeated from Primary for Secondary Tertiary Peers when retries occur based on actionset/criteriaset	Primary server header was repeated for the response from secondary and tertiary peers in a peerconfiguration where criteriaset should have matched for only Primary peer response, and only one call and one retry call should have been observed.	4	23.1.0	23.2.2

4.2.13.2 Ingress Gateway Resolved Bugs

Release 23.2.4

Table 4-52 Ingress Gateway 23.2.4 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release	Fixed in Release
35373324	HTTP/1 request are timing out with NPE after enabling HTTP/1 in IGW	The HTTP1 requests timed out with NullPointerException when HTTP1 was enabled in Ingress Gateway.	2	23.2.2	23.2.4
5409672	Routes configuration are not getting migrated from HELM to REST after upgrade	Helm routes were not migrating to REST after upgrading even though the routeConfigMode attribute was set to REST and convertHelmRoutesTo REST was set to true.	2	23.2.3	23.2.4

Table 4-52 (Cont.) Ingress Gateway 23.2.4 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release	Fixed in Release
35097588	Ingress Gateway throwing "a header value contains prohibited character 0x20 at index 0" while executing GET command using HTTPS	Ingress Gateway was neither able to send the uber-traced-id in the header nor able to create the uber-trace-id when a request didn't have a header.	3	23.1.0	23.2.4
35097588	Ingress Gateway throwing "a header value contains prohibited character 0x20 at index 0" while executing GET command using HTTPS	Ingress Gateway was neither able to send the uber-traced-id in the header nor able to create the uber-trace-id when a request didn't have a header.	3	23.1.0	23.2.4
35277831	CNCESNRF-541-NRF-IGW with message copy enabled crashes upon kafka-broker restart at OCNADD	Ingress Gateway with message copy enabled restarted when kafka-broker restarted at OCNADD. NRF was enabled with message copy at Ingress Gateway. Ingress Gateway handled 9K MPS traffic and the same was copied towards OCNADD. The kafka-brokers were scheduled for restart at an interval of 15minutes using chaosmesh. This outage restarted the NRF - Ingress Gateway pods.	2	23.1.0	23.2.3
35381653	No Configurable option for 'maxUnavailable' & 'maxSurge' during Rolling Upgrade	NSSF needed to upgrade NSSF and Ingress Gateway pods one at a time because they were facing significant traffic drop during upgrade and rollback as compared to other NFs. They needed to set maxSurge: 1 & maxUnavailable: 0 and these parameters should be exposed in the Ingress Gateway values.yaml file.	2	23.1.0	23.2.3

Table 4-52 (Cont.) Ingress Gateway 23.2.4 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release	Fixed in Release
35355832	ProvGW Ingress Gateway is throwing error : Pending acquire queue has reached its maximum size of 1000	Ingress Gateway threw an error when traffic rate was increased beyond 1000 to 1100 TPS while running SOAP traffic (HTTP1.1) in ProvGW using JMeter tool.	2	23.1.3	23.2.3
35371184	XfccHeaderValidationFilter order has change and is causing failures in ATS features	Some scenarios were failing because XfccHeaderValidationFilter should have validated whether the received headers were correct or not. However, the validation failed because the order of execution of this filter was changed and PostGatewayFilter ran first causing the negative tests to do the binding even when the request headers were incorrect.	2	23.2.2	23.2.3
35217532	cnPCRF 23.1.0-ingress-gateway pod in CrashLoopBack	The customer was getting timed out when they tried to install cnPCRF 23.1.0. Ingress Gateway restarted after deployment and went into crashLoopback state.	2	23.1.0	23.2.0
34710690	microservices traces are not correlated in Jaeger UI	When traces were queried on JAEGER UI, one single trace should have been returned with multiple spans from the different microservices involved in a single transaction. This correlation was not happening and every microservice generated a different trace.	2	22.3.4	23.2.3
34838890	No Configurable option for 'maxUnavailable' during Rolling Upgrade	Gateway Common Service charts didn't have the option to configure the maxUnavailable percentage during upgrade.	3	22.4.0	23.2.3

Table 4-52 (Cont.) Ingress Gateway 23.2.4 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release	Fixed in Release
35309236	Enabling enableTLSIncomingHttp1 does not open a new port and Ingress Gateway crashes	Ingress gateway restarted when the enableTLSIncomingHttp1 parameter was enabled, and a new pod didn't open.	3	23.1.0	23.2.3
35097588	IGW and EGW are not sending uber-traced-id in header.	Ingress Gateway didn't send uber-traced-id in header and didn't create the uber-trace-id when a request didn't have a header.	3	23.1.0	23.2.2
34610824	Message copy- Data sent to Kafka does not contain multiple via header values	The message copy data sent to Kafka didn't contain multiple via header values.	3	22.3.0	23.2.2
35104554	Upgrade is not working from 22.1.0 to 22.4.0	After successfully upgrading from 22.1.0 to 22.4.0, the customer was unable to receive provisioning requests. Requests were failing at Ingress Gateway and not getting forwarded to backend microservices.	3	22.4.0	23.2.0
34847460	Remove 1xx ,2xx ,306,599 from the IGW error code list	The error codes 1xx and 2xx should not have been used as error codes and 306 and 599 became obsolete. As a resolution, they were removed from the Ingress Gateway error code list.	3	22.4.0	23.2.0
35014846	Observing Cancellation Exception in IGW and 503 Service unavailable on EGW of 23.1.0 images which corresponds to 23.1.0 release.	Cancellation exception was observed in Ingress Gateway release 23.1.0.	3	23.1.0	23.2.0
35178640	Getting warning during helm install for ingress, egress and alternate route services	The customer was getting a warning on CNE version 22.3.0-rc.2 and and Kubernetes version v1.23.7 when they performed a helm install for Ingress Gateway.	3	23.1.0	23.2.0

Table 4-52 (Cont.) Ingress Gateway 23.2.4 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release	Fixed in Release
34708261	adding x-request-id in the IGW/EGW logs for easy co-relation with sidecar container log	Gateway Services provided ocLogId for correlation between the logs generated between NF microservices. However the container required to correlate between the Sidecar message and the application was missing. As a temporary workaround, NF used timestamps, however that wasn't sustainable during performance load. As a resolution, the container was provided. Sidecar container raised x-request-id and added it to a header for tracing the message across multiple pods. This header value was added in log messages as an attribute for debugging.	4	22.3.0	23.2.0
34930585	Gateway sending "5g-sbi-message" with a New line and Tabs (\n & \t) on Kafka	The 5g-sbi-message sent at Kafka(for both call flows and Erroneous Scenarios) when Message copy was enabled on all Gateways was sent along with special characters such as new line and tabs "\", "\n", "\t" etc along with the "5g-sbi-message".	4	22.4.1	23.2.0

4.2.13.3 Alternate Route Service Resolved Bugs

Release 23.2.3

Table 4-53 Alternate Route Service 23.2.3 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release	Fixed in Release
35381653	No Configurable option for 'maxUnavailable' & 'maxSurge' during Rolling Upgrade	NSSF needed to upgrade NSSF and Ingress Gateway pods one at a time because they faced significant traffic drop during upgrade and rollback as compared to other NFs. They needed to set maxSurge: 1 & maxUnavailable: 0 and these parameters should be exposed in the Alternate Route Services values.yaml file.	2	23.1.0	23.2.3
34838890	No Configurable option for 'maxUnavailable' during Rolling Upgrade	Gateway Common Service charts didn't have the option to configure the maxUnavailable percentage during upgrade.	3	22.4.0	23.2.3
35178640	Getting warning during helm install for ingress, egress and alternate route services	The customer was getting a warning on CNE version 22.3.0-rc.2 and Kubernetes version v1.23.7 when they performed a Helm install for Alternate Route Services.	3	23.1.0	23.2.0

4.2.13.4 ATS Resolved Bugs

Table 4-54 ATS 23.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35174715	NSSF ATS 23.1.0: unable to configure pipeline.	The user was unable to save the modified configurations in the pipeline before triggering a build, and an HTTP 403 error was received after selecting the Save option.	2	23.1.0

Table 4-54 (Cont.) ATS 23.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35124412	403 Response received while saving ATS pipeline configuration	When saving the ATS pipeline configurations, a 403 error response was received.	3	23.1.0
35078521	Getting ATS Authentication failure while using ATS base image-23.1.0 in 22.4.0 CNE setups	During the triggering of new feature and regression jobs, an authentication failure issue was encountered. This issue occurred when the latest ATS base image, version 23.1.0, was used to run on CNE version 22.4.0.	3	22.4.0
34609837	Jenkins doesn't list test cases when scenario outlines are used	When scenario outlines were used in a feature file, Jenkins was unable to list the test cases when the feature was selected.	3	22.1.0
35081861	Jenkins displays success status even if execution stopped due to behave being killed abruptly	Jenkins occasionally printed the build status as success when the build run wasn't completed rather than reporting it as a "unstable build" when the BEHAVE process was suddenly terminated.	3	23.1.0
35217837	PCAP Logs are not collecting when the helm release name has 'ocats' in its	PCAP logs were not collecting logs when the helm release name contained "ocats" in it.	3	23.1.0
35366902	Jenkins logo showing instead of Oracle logo in ATS GUI	The Jenkins logo was visible at the tab level when the ATS GUI was accessed in the Google Chrome browser. The Jenkins logo and the messages "Please wait while Jenkins is restarting" and "Your browser will reload automatically when Jenkins is ready" appeared on the loading page when Jenkins was restarted or opened for the first time.	3	23.1.0
35366897	Issues in ATS GUI with FireFox	Significant problems occurred when the ATS GUI opened in the Firefox browser.	4	23.1.0

4.3 Known Bug List

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

4.3.1 BSF Known Bugs

BSF 23.2.4 Known Bugs

There are no new known bugs in this release. Known bugs from 23.2.x have been forward ported to release 23.2.4.

Table 4-55 BSF 23.2.3 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36000199	spring.cloud.kubernetes.discovery.isIpv6Setup flag is not added in bsf-mgmt deployment in BSF	The spring.cloud.kubernetes.discovery.isIpv6Setup flag is not available in BSF Manamement deployment from BSF 23.2.x.	In a pure IPv6 non dual stack environment, audit validation of PCF binding records towards PCF is affected. **Workaround**: User can enable IPv6 manually in BSF Management deployment by adding the following field in the BSF Management deployment: `name: spring.cloud.kubernetes.discovery.isIpv6Setup value: "true"`	3	23.2.3

> **Note:**
>
> Known bugs from 23.2.x have been forward ported to Release 23.2.3.

BSF 23.2.2 Known Bugs

There are no new known bugs in this release. Known bugs from 23.2.x have been forward ported to release 23.2.2.

BSF 23.2.1 Known Bugs

There are no new known bugs in this release. Known bugs from 23.2.0 have been forward ported to release 23.2.1.

BSF 23.2.0 Known Bugs

There are no new known bugs in this release. Known bugs from 23.1.x have been forward ported to release 23.2.0.

4.3.2 CDCS Known Bugs

CDCS 23.2.2 Known Bugs

Table 4-56 CDCS 23.2.2 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 user.	Installation of CNE using CDCS fails when the installation is performed using a username other than cloud-user on the Bastion Host. **Workaround**: Provide the correct permissions for new user.	3	23.2.0	Users will be limited to use only one user while deploying CNE.

CDCS 23.2.1 Known Bugs

There are no known bugs in this release.

CDCS 23.2.0 Known Bugs

There are no known bugs in this release.

4.3.3 CNC Console Known Bugs

CNC Console 23.2.2

There are no known bugs in this release.

CNC Console 23.2.1

There are no known bugs in this release.

CNC Console 23.2.0

There are no known bugs in this release.

4.3.4 cnDBTier Known Bugs

Table 4-57 cnDBTier 23.2.5 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	After an upgrade to cnDBTier 23.2.2, all ndbmysqld pods restart frequently.	ndbmysqld georeplication pods restart as the binlog injector thread gets stalled. However, there is no impact to customer traffic due to the restarts of these pods. **Workaround**: Restart the ndbmysqld georeplication pods when bin log injector thread gets stalled such that there is no impact on the customer traffic.	1	23.2.2

cnDBTier Release 23.2.4

There are no known bugs in this release.

cnDBTier Release 23.2.3

There are no known bugs in this release.

cnDBTier Release 23.2.2

There are no known bugs in this release.

cnDBTier Release 23.2.1

There are no new known bugs in this release. For existing known bugs, see cnDBTier 23.2.0 Known Bugs.

cnDBTier Release 23.2.0

Table 4-58 cnDBTier 23.2.0 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

35561614	DBTier 23.2.0 high number of writes when Inframonitor PVC Health Enabled	High disk writes are observed when the PVC monitoring feature is enabled. That is the PVC Monitoring feature increases the PVC load in cnDBTier.	High load on PVC increases the disk pressure and impacts the performance.
			Workaround:
			Update the `custom_values.yaml` file with the following changes and perform an Helm upgrade.
			
			`mgm:`
			`  inframonitor:`
			`  command:`
			`  dd_bs: "2K"`
			`  dd_count: "2"`
			`ndb:`
			`  inframonitor:`
			`  command:`
			`  dd_bs: "2K"`
			`  dd_count: "2"`
			`api:`
			`  inframonitor:`
			`  command:`
			`  dd_bs: "2K"`
			`  dd_count: "2"`
			`  ndbapp:`
			`  inframonitor:`
			`  command:`
			`  dd_bs: "2K"`
			`  dd_count: "2"`
			
			This configuration will write 4 KB of data for every 15 seconds.
				2	23.2.0

Table 4-58 (Cont.) cnDBTier 23.2.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35590372	cnDBTier 23.2.0 MIBs and alertrules don't match	cnDBTier 23.2.0 Management Information Base (MIBs) and alertrules are not matching.	The module identity defined in the MIB template doesn't match with the Object Identifiers (OIDs) of the alerts. As a result, Simple Network Management Protocol (SNMP) is unable to trap any alert raised by the system leading to missing traps that are collected. **Workaround**: • Update the configuration in `occndbtier_mib.mib`: 1. Open the `occndbtier_mib.mib` file in the `<CSAR_FILE_EXTRACTED>/Artifacts/Scripts/snmp_mibs` folder. 2. Update the configuration in line number "44" from `::= { oracleDbTier 2 }` to `::= { oracleDbTier 1 }` • Update the configuration in `occndbtier_mib_tc.mib`: 1. Open the `occndbtier_mib_tc.mib` file in the `<CSAR_FILE_EXTRACTED>/Artifacts/Scripts/snmp_mibs` folder. 2. Update the configuration in line number "43" from `::= { oracleDbTier 2 }` to `::= { oracleDbTier 1 }`	3	23.2.0

Table 4-58 (Cont.) cnDBTier 23.2.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release

35909630	cnDBTier 23.2.1 software packaging issue	The occndbtier_mysqlndb_vnfd.yml file in CSAR package is incorrect.	Orchestrator fails to install cnDBTier.
			Workaround:
			Make the following updates on the `/Definitions/occndbtier_mysqlndb_vnfd.yml` file:
			1. Update the `custom_values.yaml` file name in the `topology_template.node_templates.occndbtier_helm.artifacts.values.yaml` section:
			`values.yaml:`
			`file: /Artifacts/Scripts/occndbtier_custom_values_23.2.0.yaml`
			`type: tosca.artifacts.File`
			2. Add the following configurations in the end of the `topology_template.node_templates.occndbtier_helm.artifacts` section:
			`occne-db-infra-monitor-svc:`
			`file: /Artifacts/Images/occne-db-infra-monitor-svc-##DBTIER_IMAGES_VERSION.tar`
			`type: tosca.artifacts.nfv.SwImage`
				3	23.2.1

4.3.5 CNE Known Bugs

Table 4-59 CNE 23.2.6 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 are 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	3	23.2.0

Table 4-59 (Cont.) CNE 23.2.6 Known Bugs

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

CNE 23.2.5 Known Bugs

There are no new known bugs in this release. For existing known bugs, see CNE 23.2.1 Known Bugs.

CNE 23.2.4 Known Bugs

There are no new known bugs in this release. For existing known bugs, see CNE 23.2.1 Known Bugs.

CNE 23.2.3 Known Bugs

There are no new known bugs in this release. For existing known bugs, see CNE 23.2.1 Known Bugs.

Table 4-60 CNE 23.2.1 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 doesn't transition states. This bug was 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 23.2.x, configure the index management policy for OpenSearch Dashboard after the installation. For procedure, see the "Verifying and Configuring Common Services" section in *Oracle Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide*. If you are upgrading from 23.1.x to 23.2.x, configure the index management policy for OpenSearch Dashboard before performing an upgrade. For procedure, see the "Configuring Index	2	23.1.1

Table 4-60 (Cont.) CNE 23.2.1 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
			Management Policy for OpenSearch Dashboard" section in *Oracle Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide*.		

Table 4-60 (Cont.) CNE 23.2.1 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 are 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 4-61 CNE 23.2.0 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 doesn't transition 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 23.2.x, configure the index management policy for OpenSearch Dashboard after the installation. For procedure, see the "Verifying and Configuring Common Services" section in *Oracle Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide*. If you are upgrading from 23.1.x to 23.2.0, configure the index management policy for OpenSearch Dashboard before performing an upgrade. For procedure, see the "Configuring	2	23.1.1

Table 4-61 (Cont.) CNE 23.2.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
			Index Management Policy for OpenSearch Dashboard" section in *Oracle Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide*.		

Table 4-61 (Cont.) CNE 23.2.0 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 are 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 23.2.0

There are no known bugs in this release.

4.3.6 NEF Known Bugs

NEF Release 23.2.1

There are no known bugs in this release.

NEF Release 23.2.0

There are no known bugs in this release.

4.3.7 NRF Known Bugs

NRF 23.2.3 Known Bugs

There are no new known bugs for this release. For the existing known bugs, see Table 4-62.

NRF 23.2.2 Known Bugs

There are no new known bugs for this release. For the existing known bugs, see Table 4-62.

NRF 23.2.1 Known Bugs

There are no new known bugs for this release. For the existing known bugs, see Table 4-62.

Table 4-62 NRF 23.2.0 Known Bugs

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

Table 4-62 (Cont.) NRF 23.2.0 Known Bugs

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

Table 4-62 (Cont.) NRF 23.2.0 Known Bugs

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

Table 4-62 (Cont.) NRF 23.2.0 Known Bugs

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

4.3.8 NSSF Known Bugs

Table 4-63 NSSF 23.2.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35183920	Ingress pod memory gradually increasing while running traffic with 2.5K TPS with NSSF 23.1.0	In a long run of performance, post 12 to 14 hours, an increase in RAM utilization is being observed at NsSelection Ingress Gateway.	The increase in memory utilization is minimal and under control. **Workaround**: No workaround available	3	23.1.0
35368703	NSSF is not sending the taiRangeList in Notifications, if Ns-availability Update request for same taiRangeList	Intermittently for scenarios where subscription is for multiple taiRanges and Configuration also contains intersecting tai ranges. In the event of NsAvailabilityInfo with tai ranges overlapping with the one in subscription and configuration. If AMF is either the first AMF to support a Ta–SNSSAI combination that is not supported by any other AMF in the network, then the notification missed this information.	There is minimal loss of service as this is an intermittent issue over a corner-case scenario. **Workaround**: No workaround available	3	23.1.0
35368483	NSSF should reject the roaming scenarios because of roaming is not supported	NSSF does not support Roaming use cases. IEs (optional) corresponding to roaming are ignored at NSSF.	There is no loss of service as the SBI message is not impacted. The additional IEs are ignored. **Workaround**: No workaround available	3	23.1.0

Table 4-63 (Cont.) NSSF 23.2.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35322891	Selection pod restart observed during traffic run 10K with NSSF version 23.1.1	In a long run of performance for 6 days, on the third day, a NsSelection pod got restarted. This has happened only once and has happened with only one Pod of NsSelection.	The restart was due to the pod going out of memory. All other pods of NsSelection resources were within limits. This happened on the third day only in one case in the long run and this did not get replicated. **Workaround**: No workaround available	3	23.1.1

Table 4-63 (Cont.) NSSF 23.2.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35006416	NS-Availability data should not deleted in database which running patch NS-Availability scenarios	NS-Availability data should not be deleted in the database which runs patches for NS-Availability scenarios.	T he impact is low as the scenario is a rare event. During NsAvailability patch processing, the content of provision data is updated. The update occurred only in those scenarios if that is the only AMF in the whole network supporting a particular SNSSAI in a TAI. In the real world, the use case of a single AMF (not AMF-Set) supporting an SNSSAI in a TAI is a rare scenario. If any other AMF sends a NsSelection request for that same Tai-SNSSAI combination, this adds to the make this more corner case. Also, only during the transition time when patch processing is being done, there are chances for data loss in the SBI message. **Workaround**: No workaround available	3	22.4.1

Table 4-63 (Cont.) NSSF 23.2.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35381963	nsconfig service option is not visible while saving the log level options "NSSF->Log Level Option"	The nsconfig service option is not visible while saving the log level options "NSSF->Log Level Option".	There is no loss of traffic 5G-SBI messages.The operator will not be able to update the log level of the NsConfig microservice at run time. **Workaround**: No workaround available	3	23.1.1
35368636	NSSF is sending the Multiple Notifications, when Ns-availability Update request for same taiRangeList	Intermittently in a scenario where subscription is for multiple taiRanges and Configuration also contains interesting tai ranges. The Notification message (only in case the trigger for notification is NsAvailability info) sends multiple notifications.	Multiple notifications can impact AMF as more processing is to be done. The traffic impact is low as the scenario is a corner case, and this happens intermittently. **Workaround**: No workaround available	3	23.1.0
35352648	NSSF is sending the failure for supportedNssaiAvailabilityData.taiRangeList.tacRangeList.patternIE.	NSSF does not support optional parameter patterns, which are part of TaiRangeList.	No customer impact **Workaround**: Use a combination of Start and End to identify a tac range.	3	23.1.0
35395855	NSSF (Discovery request) is not retrying the discovery request towards NRF for failure scenario.	In the case of the configuration of AMF set when a response from discovery is an error and the MaxRetys parameter (helm configuration) is set to 1, there are no retries from NsConfig.	No 5G SBI call flow is impacted. **Workaround**: This call flow is during configuration. The operator will have to retry the configuration of the AMF Set.	3	23.1.0

Table 4-63 (Cont.) NSSF 23.2.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35377428	Unable to find out some subscription and discovery NRF metrics in prometheus	The metrics peg is missed in one scenario of configuration.	There is no loss of traffic as the call flow is not impacted. The user is unable to validate the count of messages from NsConfig to Nrf. **Workaround**: No workaround available	3	23.1.0
35395810	When set nsconfig.httpMaxRetries to 3, NSSF (Discovery request) is sending 3 times towards NRF for success scenario.	When the operator is configuring the AMF set, NSSF sends a Discovery request to NRF. When the Max Retry parameter is set to 3 in case of success also there are 3 retrials.	There is no loss of traffic and there are two additional messages in the network (retrials in success case), since operator configuration of AMF set is a rare occurrence. The impact on the network is minimal.	3	23.1.0

Table 4-63 (Cont.) NSSF 23.2.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35396406	NSSF is sending the incorrect value of NRFNFmanagement IE and nrfAmfSetAccessTokenUri IE in ns-selection response.	In scenarios where NSSF is not sending proper value, there are optional IEs in case of the initial registration request.	The impact is minimal to low. These parameters are not mandatory. The discovery URL is being sent properly, which manages the AMF handover. In scenarios where authorization is mandatory and AMF does not send a discovery, the handover scenario will get impacted. **Workaround**: While configuring the NSI profile, the operator can configure the Management URI of NRF at both Management and AccessToken URI.	3	23.1.1

Table 4-63 (Cont.) NSSF 23.2.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35388661	NsAvailabilityInfo PUT call flow is taking more than 100ms	NsAvailabilityInfo PUT call flow is taking more than 100ms.	There is no loss of messages. The issue is higher latency. In rare case scenarios, this can be a setup constraint. The latency is appropriate for the same test scenario in case the underlying setup is bare metal CNE. Since this is a vCNE setup, there is an impact on latency and resource consumption. **Workaround**: This issue is not observed in bare metal setups. Moving to a bare metal setup increases cnDBTier resources.	3	23.1.1
35208077	Selection pod memory gradually increasing while running traffic with 2.5K TPS with NSSF 23.1.0	In a long run of performance post 12 to 14 hours, an increase in RAM utilization is being observed at NsSelection Ingress Gateway.	The increase in memory utilization is minimal and is under control. **Workaround**: No workaround available	4	23.1.0

Table 4-63 (Cont.) NSSF 23.2.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
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. There is a difference in specifications if both must be supported or not. Since the support is there for both and each parameter is separate, there is no loss of traffic.	There is no loss of traffic. **Workaround**: No workaround available	4	23.1.0
35394240	CandidateAmfList is not added by NSSF when No AMF is sending the ns-availability update request to NSSF	This is a corner case where no AMF in the network is providing an Availability Update.	1. PLMN Level Profile (Default profile) is being mapped to an operator-configured rule. 2. No AMF is sending availability updates. Because of this, there is no mapping of AMF set to that profile. 3. This leads to a situation where no AMF set is linked. **Workaround**: The operator must configure Rule and Map with a Network Slice profile rather than a default PLMN profile.	4	23.1.0

Table 4-63 (Cont.) NSSF 23.2.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35394355	Error details should be same for ns-availability update and subscription request, if ONSSAI disabled in NSSF	The error detail field is not the same for the missing mandatory parameters in the case of the subscription message and AvailabilityInfo message.	There is no impact as the return code and cause code are the same and valid. **Workaround**: No workaround available	4	23.1.0

4.3.9 Policy Known Bugs

Policy 23.2.8 Known Bugs

There are no new known bugs in this release. Known bugs from 23.2.x have been forward ported to Release 23.2.8.

Policy 23.2.7 Known Bugs

There are no new known bugs in this release. Known bugs from 23.2.x have been forward ported to Release 23.2.7.

Policy 23.2.6 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35859214	[pcf-audit] If compression is enabled in 23.2.6 and post rollback from 23.2.6 to 23.1.7(compression disabled) audit is not working for SM service	If db compression is enabled in Policy 23.2.6, after rolling back from Policy 23.2.6 to 23.1.7, if db compression is disabled, audit does not work for SM service.	If db compression is enabled post upgrade and it is disabled after rolling back, the audit does not work for the records that have a mismatch in the V column and COMPRESSION_SCHEME column. **Workaround**: Manually delete the records that have a mismatch in the V column and COMPRESSION_SCHEME column.	3	23.1.7

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36018490	UE service not adding 3GPP-sbi-binding header to n1-n2 transfer retransmission message on T3501 timer expiry	When **Send SBI Binding Header For N1N2 Transfer Requests** field is configured for UE Policy service, if the binding information changes after a UE create request is complete, during UE update or UDR notification when UE Policy service triggers N1-N2 transfer messages, the 3GPP-sbi-binding header is present. But, when N1-N2 transfer message is retransmitted again on T3501 timer expiry, the 3GPP-sbi-binding is missing in N1-N2 Transfer message. Retransmission message should be the same as it was sent earlier.	Binding header is missing in the retransmission message during N1-N2 transfer, which is required by AMF for subsequent usage. **Workaround**: NA	3	23.2.6
36018660	[pcf-audit]: Post rollback pcf-am audit registration is not updated	After rolling back from Policy 23.2.6, the audit registration for AM service is not updated.	Stale audit registration from the upgraded release is present. **Workaround**: Disable and then enable Audit service in order to refresh the audit registration.	3	23.2.6

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36018805	[pcf-audit]: Post upgrade from 23.2.4 to 23.2.6-rc3 pcf-am audit registration is not updated	Post upgrade from 23.2.4 to 23.2.6, audit registration for AM service is not updated. All the re-attempts to update audit registration are done within a short duration and audit registration is not attempted further.	Audit registration data is not updated for AM service. **Workaround**: Disable and then enable Audit service in order to refresh the audit registration.	2	23.2.6
36018809	UE N1N2 Transfer Session Retry Not Working based on available AMFs.	Session retry for N1N2 Transfer message does not work based on AMF discovered data, when DNS fall back is enabled. An alternate AMF is selected for message retry. But, the alternate AMF selection based on AMF discovered data does not work.	When binding header is missing in the response from AMF to a Subscribe request, transfer message retry does not happen based on the NF set information contained in the AMF profile. If DNS Srv is enabled, retry logic works based on the DNS Srv. If "Use Binding Information from NF Profile" is disabled, then there will be no impact. **Workaround**: No workaround available.	2	23.2.4

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35992941	AM-UE: PDS is reporting SQLSyntaxErrorException: Unknown column 'pdssubscri0_.compression_scheme'	During the call flow to Bulwark service from AM service or UE Policy service, PDS reports "SQLSyntaxErrorException: Unknown column 'pdssubscri0_.compression_scheme'" error.	PDS logs are flooded with SQLSyntaxErrorException: Unknown column 'pdssubscri0_.compression_scheme' causing call failures. **Workaround**: Restart the pods in which MySQL pods data is not synchronized.	2	23.2.4

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36018814	PARTIAL_SUCCESS in Bulk Export in freshly install build in 23.4.0-nb-20230926	During fresh installation, bulk import completes with PARTIAL_SUCCESS.	Policy export shows 'partial success' in 23.2.4 and the export report is specifically complaining about the export not done for 'PCF Session Management'' page. This 'partial success' is due to the reason that 'PCF Session management' configuration was never configured in CNC Console and the default values being configured causes issues during export (these default values are not present in the database by default, although they are visible statically in CNC Console). **Workaround**: Open PCF Session Management page under Service Configurations in CNC Console and click Save button (without making any change) to persist the default configuration in the database. With this, the next export will show 'Success' for 'PCF Session	3	23.2.4

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
			Management' page as well.		
36018817	AM Service: "Error in PRE POST request:Max requests queued per destination 1024 exceeded for HttpDestination " observed when utilization of PRE is just at 20%	During AM service or UE Policy service calls, "Error in PRE POST request:Max requests queued per destination 1024 exceeded for HttpDestination " error is observed continuously at 30K TPS after 30 minutes run.	AM service flooded with errors causing calls to fail after a longer duration. **Workaround**: Use HorizontalPodAutoscaler (HPA) during execution at 30K.	2	23.2.6
35975044	PCF is unable to send SMF Notification retry request when irrelevant configuration is not set in retry profile.	PCF is unable to send SMF Notification retry request. The following error is observed in the SM service logs, which suggests that nfSetResolution value under RETRY profile should not be empty. During SMF retry, it is expected to fall back to the DNS/SRV. For this fallback scenario, nfSetResolution value is irrelevant and is configured as empty (not chosen any value from the drop down).	Fall back on DNS-SRV will not work if "NF Set Resolution" filed is empty. **Workaround**: As fallback on DNS-SRV feature is not dependent on "NF Set Resolution Set", configure "NF Set Resolution" to the default value: "Cached NF Profiles**".**	2	23.2.6

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36018826	PARTIAL_SUCCESS observed when performing Bulk Import in 23.2.6 upgraded build	After upgrading from Policy 23.2.4 to 23.2.6, bulk import completes with PARTIAL_SUCCESS.	The I/O timeout issue is observed only for 15 Policy Projects. If the number of projects is less than 15, the issue is not observed after several successive retries. **Workaround**: Use less than 15 projects.	3	23.2.6

Policy 23.2.5 Known Bugs

There are no new known bugs in this release. Known bugs from 23.2.4 have been forward ported to Release 23.2.5.

Table 4-64 Policy 23.2.4 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35575690	UDR connector prompting Error "Caught Exception while DELETE"	When the PCF receives relative URI (Unified Resource Identifier) in the location header of the response to create subscription request, UDR connector fails with NPE (NullPointerException) when it tries to send subsequent request (delete or update) for the same subscription.	Stale subscriptions are getting built up as there are no delete subscriptions from PCF. **Workaround**: No workaround available.	2	22.3.1

Table 4-64 (Cont.) Policy 23.2.4 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35877549	Replication break observed between site1 and site4 during CNDB upgrade.	Database replication is failing in a four-site setup during Policy or cnDBTier upgrade and installation, even when there is no traffic.	In a scenario where no traffic is running and has "ALTER" command in SQL statement during Upgrade or fresh installation, epoch value is resetting to zero between cnDBTier pod failover resulting in replication going down. **Workaround**: No workaround available.	2	23.2.4
35339370	PROD PCF ocpm_ingress_response_total Does not show failures for UE and AM Policy	PCF AM dashboard in Grafana under AM/UE Policy metrics does not display the failures. They are only displayed under the Ingress Gateway metrics.	For the error response from AM and UE, there are no metrics. **Workaround**: No workaround available.	3	22.3.2
35861744	"ocpm_ar_request_total" and "ocpm_ar_response_total" pegged twice with wrong context	"ocpm_ar_request_total" and "ocpm_ar_response_total" are pegged with wrong context.	ocpm_ar_request_total and ocpm_ar_response_total will get pegged during initial DNS discovery of Routes and the metric will get pegged as UE NAS context even for AMF. **Workaround**: No workaround available.	3	23.2.3

Note:

Known bugs from 23.2.2 have been forward ported to Release 23.2.4.

Table 4-65 Policy 23.2.2 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35729506	Binding SVC is not taking BSF profile in db and not reject request	When BSF is enabled and Binding service request is received, BSF returns null value despite the BSF profile exists in the database. Moreover, it does not reject the SM session.	When Binding service receives a request to create binding, BSF is returning null value despite the database contains the BSF profile, and it does not abort the session even if the configuration is enabled. **Workaround**: No workaround available.	3	23.1.7

> **Note:**
>
> Known bugs from 23.2.1 have been forward ported to Release 23.2.2.

Policy 23.2.1 Known Bugs

There are no new known bugs in this release. Known bugs from 23.2.0 have been forward ported to Release 23.2.1.

Table 4-66 Policy 23.2.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35521242	PCF: Session Retry - Service name is unavailable	During the session retry for alternate NF selection, service level parameters such as host and port are selected if service name is unavailable.	When different service instances use different scheme and port during notification retry, notifications might not reach the correct FQDN and port and the retried notification fails. **Workaround**: No workaround available.	3	23.2.0

Table 4-66 (Cont.) Policy 23.2.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35521303	PDS not sending DataSourceRouteInfo	PDS is not sending DataSourceRouteInfo to UDR connector while patch request for RemoteSSV.	If discovery is enabled before every PATCH query to UDR, then PCF carries out NRF discovery and identifies the UDR to which the UDR PATCH query needs to be sent. **Workaround**: No workaround available.	3	23.2.0
35521348	Usage-mon: Subscriber-Remote Variable	For Usage Monitoring: PATCH request with Remove Subscriber-Remote variable sent from PDS to UDR does not remove the variable in UDR.	Remove Subscriber Remote variable does not remove the variable at UDR. This leads to failure of Policy decision that is made based on the missing variable in UDR. **Workaround**: Instead of removing the variable, set the variable at UDR to a value that is equivalent to null.	3	23.2.0
35521348	Bulk Export	Bulk export from Policy 23.1.3 does not export the complete configuration when the Policy project is more than 15 MB in size.	User cannot export the data if the data size is 15 MB or more. This happens when user has created large set of policy projects, which are clone of each other. It is observed that at a time only one Policy Project can be in Prod state. **Workaround**: User can delete the Policy Projects that are not used or not needed any more. User can use the option to Select the Policy Project and its dependency for Export. This way Policy Projects can be exported separately.	3	23.2.0

Table 4-66 (Cont.) Policy 23.2.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35521311	UDR PUT request is sent to GET successful UDR	UDR PUT request is sent to GET successful UDR instead of POST successful UDR.	PUT request on UDR may be made on incorrect UDR insted of previous POST success UDR in revalidated Subscription cases. **Workaround**: No workaround available	3	23.2.0
35521426	UDR PATCH session-retry is not working	UDR PATCH session-retry is not working.	Patch request for Remote SSV update on UDR will be impacted including Session Retry as for each Patch request in case of remote SSV, new UDR discovery and reselection will happen and request may be directed to different UDRs instead of the UDR that was selected during initial GET request. **Workaround**: No workaround available	3	23.2.0

Note:

Known bugs from 23.1.x have been forward ported to Release 23.2.0.

4.3.10 SCP Known Bugs

SCP 23.2.3 Known Bugs

There are no new known bugs in this release. For existing known bugs, see Table 4-67.

SCP 23.2.2 Known Bugs

There are no new known bugs in this release. For existing known bugs, see Table 4-67.

SCP 23.2.1 Known Bugs

There are no new known bugs in this release. For existing known bugs, see Table 4-67.

Table 4-67 SCP 23.2.0 Known Bugs

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

4.3.11 SEPP Known Bugs

SEPP 23.2.2 Known Bugs

There are no new known bugs in this release. Known bugs from 23.2.0 have been forward ported to Release 23.2.2.

SEPP 23.2.1 Known Bugs

There are no new known bugs in this release. Known bugs from 23.2.0 have been forward ported to Release 23.2.1.

Table 4-68 SEPP Release 23.2.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
35036599	Total traffic loss after upgrade when global Ingress rate limiting feature is enabled	There is a total traffic failure when SEPP is upgraded from 22.3.x, 224.x to 23.1.0, and the global rate limiting feature is enabled. The following exception is displayed 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) The traffic is normal, if the Ingress pod is restarted.	If the Global Ingress Rate Limiting feature is enabled and the network traffic is ongoing and the upgrade is performed to 22.4.x or 23.1.0 release, then after the upgrade n32-ingress-gateway stops processing traffic. There will be total loss of the traffic. **Workaround**: The following workarounds can be used: • If SBI traffic is ongoing during the upgrade, then after the upgrade, restart the n32-ingress-gateway. System will recover and start processing traffic. • Perform the upgrade with	2	22.4.0

Table 4-68 (Cont.) SEPP Release 23.2.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
			Global Rate Limiting feature sets disabled. • Perform the upgrade to 23.1.0 without traffic.		
34569424	Proper error reason must be displayed by C-SEPP when n32-ingress service is scaled down at P-SEPP and an interplmn request is sent from C-SEPP to P-SEPP.	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. - HTTP error status in response received by gateway and the details can be configured through values.yaml file - Code exception mentioned in error-reason is coming from Egress Gateway code error reason: org.springframework.web.reactive.function.client.WebClientRequestException:nested exception is java.nio.channels.ClosedChannelException API Gateway bug 34737029 is raised.	The user cannot identify the reason of failure from the error description. The user has to check the grafana and metrics to find the root cause. **Workaround**: Run the kubectl command to verify that all the services are up and running. Wait for the service to come up and issue will get resolved.	3	22.2.0

Table 4-68 (Cont.) SEPP Release 23.2.0 Known Bugs

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

Table 4-68 (Cont.) SEPP Release 23.2.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
34374452	SEPP-COM-xx-ERROR-0103 not observed when n32c pods have been scaled down	On scaling down pn32c and cn32c pods, if a Delete request is run for the configured remotesepp, error code 204 is returned but the entry is not deleted. Also, no error is displayed when POST request is run, when the pods are scaled down.	There is no impact. **Workaround**: Ensure that the the pod and services are up. Run the command and it will be run successfully.	4	22.3.0
35208390	cn32f and pn32f pods restart observed during cnDBTier rollback from 23.1.0 to 22.4.0	The restarting of cn32f and pn32f pods is observed during cnDBTier rollback from 23.1.0 to 22.4.0.	The restarting of cn32f and pn32f pods is observed during cnDBTier rollback from 23.1.0 to 22.4.0. **Workaround**: No workaround available	3	23.1.0
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 or 22.3.x, some of the table data gets replicated. This is the data which is either removed or updated during upgrade.	Some of the tables will show duplicated extra data. **Workaround**: No workaround available	3	23.2.0

4.3.12 UDR Known Bugs

UDR 23.2.2 Known Bugs

There are no new known bugs in this release. Known bugs from 23.2.0 have been forward ported to Release 23.2.2.

UDR 23.2.1 Known Bugs

There are no new known bugs in this release. Known bugs from 23.2.0 have been forward ported to Release 23.2.1.

Table 4-69 UDR 23.2.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35410952	PUR update of state data is not generating notification when subscription is created for SM-DATA	5G notification is not triggered when PUR SH request is sent to update the state data and subscription exists only for 5G data	For the converged UDR case, SNR needs to be sent and subs-to-notify also for 5G Data. If subscription is created on 5G data only and update comes from Diameter, notificaiton is generated. **Workaround**: Create subscription on Diameter for 4G Policy data.	3	23.2.0
35243448	DNN Validation is missing while provisioning the SM-DATA	Data Network Name (DNN) value under sm-data should have pattern validation by default.	This is not a significant issue and there is no functional impact. **Workaround**: No workaround available	3	23.1.0

Table 4-69 (Cont.) UDR 23.2.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35065447	DB Records are not sync properly after network replication recovery	In a site isolation scenario, if the provisioning requests are sent to create same subscriber having same Mobile Station Integrated Services Digital Network (MSISDN), the subscribers are created in each site in isolation. When bringing up the replication it creates inconsistent subscriber information on both the sites.	Provisioning must be done on only one site and parallel provisioning must not be done when replication is broken. **Workaround**: No workaround available	3	22.4.0
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 even when the configuration flag is set as false.	NRF management messages contain user agent header even when user agent feature is disabled. There is no functional impact. **Workaround**: No workaround available	3	22.3.1
35402560	Provgw disable jaegerTracingEnabled to stop Jaeger log collection	There is no flag to disable Jaegar tracing on performance pod.	There is no flag to disable Jaegar tracing on perf-info. **Workaround**: No workaround available	3	23.1.1

4.3.13 Common Services Known Bugs

4.3.13.1 Egress Gateway Known Bugs

Release 23.2.4

There are no known bugs in this release.

4.3.13.2 Ingress Gateway Known Bugs

Release 23.2.4

Table 4-70 Ingress Gateway 23.2.4 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35011024	Unique Key Constraint violation is happening for common_configuration and common_configuration_backup database tables	There is a limitation in the database tier on using the UNIQUE key constraint.	Mysql replication skips the epoch transaction. After the cluster disconnect, all DML statements are skipped. If any DML statement has an operation from the common_configuration and common_configuration_backup tables, the user may face issues because it is difficult to identify the DML statements that were skipped in the past. **Workaround**: As a workaround, the customer needs to add 1022 error code inSkip Slave Errors so that the replication link doesn't break.	3	22.3.0

4.3.13.3 Alternate Route Service Known Bugs

Release 23.2.3

There are no known bugs in this release.

4.3.13.4 ATS Known Bugs

Release 23.2.0

There are no known bugs in this release.