Oracle® Communications

Cloud Native Core Release Notes

Release 2.22.3
F69946-26
January 2023

Oracle Communications Cloud Native Core Release Notes, Release 2.22.3

F69946-26

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 2.22.3 - F69946-26, January 2023

Updated the following sections with the details of CNC Policy 22.3.4 Release:

- Media Pack: Updated the media pack details for CNC Policy release 22.3.4.
- Compliance Matrix: Updated the compliance matrix information for CNC Policy release 22.3.4.
- Common Microservices Load Lineup: Updated the common services load lineup details for CNC Policy release 22.3.4.
- Security Certification Declaration : Added security declaration for CNC Policy release 22.3.4.

Release 2.22.3 - F69946-26, January 2023

Updated the following sections with the details of BSF 22.3.4 Release:

- Media Pack: Updated the media pack details for BSF release 22.3.4.
- Compliance Matrix: Updated the compliance matrix information for BSF release 22.3.4.
- Common Microservices Load Lineup: Updated the common services load lineup details for BSF release 22.3.4.
- Security Certification Declaration : Added security declaration for BSF release 22.3.4.

Release 2.22.3 - F69946-25, January 2023

Updated the following sections with the details of CNE 22.3.3 Release:

- Media Pack: Updated the media pack details.
- Compliance Matrix: Updated the compliance matrix information.
- CNE Resolved Bugs: Added resolved bugs list for CNE release 22.3.3.

Release 2.22.3 - F69946-24, January 2023

CNC Console 22.3.2 Release
Updated the following sections with the details of CNC Console 22.3.2 Release:

- Media Pack: Updated the media pack details for CNC Console release 22.3.2.
- Compliance Matrix: Updated the compliance matrix information for CNC Console release 22.3.2.
- Common Microservices Load Lineup: Updated the common services load lineup details for CNC Console release 22.3.2.
- Security Certification Declaration : Added security declaration for CNC Console release 22.3.2.
- CNC Console Resolved Bugs: Added resolved bugs list for CNC Console release 22.3.2.

NEF 22.3.2 Release

Updated the following sections with the details of NEF 22.3.2 Release:

- Media Pack: Updated the media pack details for NEF release 22.3.2.
- Compliance Matrix: Updated the compliance matrix information for NEF release 22.3.2.
- Common Microservices Load Lineup: Updated the common services load lineup details for NEF release 22.3.2.
- Security Certification Declaration : Added security declaration for NEF release 22.3.2.

NRF 22.3.2 Release
Updated the following sections with the details of NRF 22.3.2 Release:

- Media Pack: Updated the media pack details for NRF release 22.3.2.
- Compliance Matrix: Updated the compliance matrix information for NRF release 22.3.2.
- Common Microservices Load Lineup: Updated the common services load lineup details for NRF release 22.3.2.
- Security Certification Declaration : Added security declaration for NRF release 22.3.2.
- NRF Resolved Bugs: Added resolved bugs list for NRF release 22.3.2.
- NRF Known Bugs: Added known bugs list for NRF release 22.3.2.

SEPP 22.3.2 Release
Updated the following sections with the details of SEPP 22.3.2 Release:

- Media Pack: Updated the media pack details for SEPP release 22.3.2.
- Compliance Matrix: Updated the compliance matrix information for SEPP release 22.3.2.
- Common Microservices Load Lineup: Updated the common services load lineup details for SEPP release 22.3.2.
- Security Certification Declaration : Added security declaration for SEPP release 22.3.2.
- SEPP Resolved Bugs: Added resolved bugs list for SEPP release 22.3.2.

UDR 22.3.4 Release
Updated the following sections with the details of UDR 22.3.4 Release:

- Media Pack: Updated the media pack details for UDR release 22.3.4.
- Compliance Matrix: Updated the compliance matrix information for UDR release 22.3.4.
- Common Microservices Load Lineup: Updated the common services load lineup details for UDR release 22.3.4.
- Security Certification Declaration : Added security declaration for UDR release 22.3.4.
- UDR Resolved Bugs: Added resolved bugs list for UDR release 22.3.4.
- UDR Known Bugs: Added resolved bugs list for UDR release 22.3.4.

Release 2.22.3 - F69946-23, January 2023

DBTier 22.3.4 Release
Updated the following sections with the details of DBTier 22.3.4 Release:

- Media Pack: Updated the media pack details for DBTier release 22.3.4.
- Compliance Matrix: Updated the compliance matrix information for DBTier release 22.3.4.
- DBTier Resolved Bugs: Added resolved bugs list for DBTier release 22.3.4.

NSSF 22.3.2 Release

Updated the following sections with the details of NSSF 22.3.2 Release:

- Media Pack: Updated the media pack details for NSSF release 22.3.2.
- Compliance Matrix: Updated the compliance matrix information for NSSF release 22.3.2.
- Common Microservices Load Lineup: Updated the common services load lineup details for NSSF release 22.3.2.
- Security Certification Declaration : Added security declaration for NSSF release 22.3.2.

SCP 22.3.4 Release
Updated the following sections with the details of SCP 22.3.4 Release:

- Media Pack: Updated the media pack details for SCP release 22.3.4.
- Compliance Matrix: Updated the compliance matrix information for SCP release 22.3.4.
- Common Microservices Load Lineup: Updated the common services load lineup details for SCP release 22.3.4.
- Security Certification Declaration : Added security declaration for SCP release 22.3.4.
- SCP Resolved Bugs: Added resolved bugs list for SCP release 22.3.4.

Release 2.22.3 - F69946-22, January 2023

Updated the following sections with the details of SCP 22.3.3 Release:

- Media Pack: Updated the media pack details for SCP release 22.3.3.
- Compliance Matrix: Updated the compliance matrix information for SCP release 22.3.3.
- Common Microservices Load Lineup: Updated the common services load lineup details for SCP release 22.3.3.
- Security Certification Declaration : Added security declaration for SCP release 22.3.3.
- SCP Resolved Bugs: Added resolved bugs list for SCP release 22.3.3.
- SCP Known Bugs: Added known bugs list for SCP release 22.3.3.

Release 2.22.3 - F69946-21, December 2022

Updated the resolved bugs list for UDR-ATS release 22.3.4 in the UDR Resolved Bugs section.

Release 2.22.3 - F69946-20, December 2022

The following sections are updated for DBTier 22.3.3:

- Media Pack: Updated media pack details for DBTier release 22.3.3.
- Compliance Matrix: Updated the compliance matrix information for DBTier release 22.3.3.
- DBTier Resolved Bugs: Added known bugs list for DBTier release 22.3.3.

Release 2.22.3 - F69946-19, December 2022

Added the resolved bugs list for UDR-ATS release 22.3.4 in the UDR Resolved Bugs section.

Release 2.22.3 - F69946-18, November 2022

Updated the resolved bugs list for NRF-ATS release 22.3.2 in the NRF Resolved Bugs section.

Release 2.22.3 - F69946-17, November 2022

Updated the following sections with the details of SCP 22.3.2 Release:

- Media Pack: Updated the media pack details for SCP release 22.3.2.
- Compliance Matrix: Updated the compliance matrix information for SCP release 22.3.2.
- Common Microservices Load Lineup: Updated the common services load lineup details for SCP release 22.3.2.
- Security Certification Declaration : Added security declaration for SCP release 22.3.2.
- SCP Resolved Bugs: Added resolved bugs list for SCP release 22.3.2.
- SCP Known Bugs: Added known bugs list for SCP release 22.3.2.

Release 2.22.3 - F69946-16, November 2022

Updated the following section with the details of Policy 22.3.3 Release:

- CNC Policy Resolved Bugs: Added resolved bugs list for CNC Policy release 22.3.3.
- CNC Policy Known Bugs: Added known bugs list for CNC Policy release 22.3.3.
- Media Pack: Updated the media pack details for CNC Policy release 22.3.3.
- Compliance Matrix: Updated the compliance matrix information for CNC Policy release 22.3.3.
- Common Microservices Load Lineup: Updated the common services load lineup details for CNC Policy release 22.3.3.
- Security Certification Declaration : Added security declaration for CNC Policy release 22.3.3.

Release 2.22.3 - F69946-15, October 2022

Updated the following section with the details of DBTier 22.3.2 Release and OSO 22.3.2 Release:

- Media Pack: Updated the media pack details.
- Compliance Matrix: Updated the compliance matrix information.
- Cloud Native Environment (CNE): Added common service versions for OSO release 22.3.2.
- CNE Resolved Bugs: Added resolved bugs list for OSO release 22.3.2.
- DBTier Resolved Bugs: Added resolved bugs list for cnDBTier release 22.3.2.

Release 2.22.3 - F69946-14, October 2022

Updated the following section with the details of Policy and BSF 22.3.2 Release:

- CNC Policy Resolved Bugs: Added resolved bugs list for CNC Policy release 22.3.2.
- CNC Policy Known Bugs: Added known bugs list for CNC Policy release 22.3.2.
- BSF Resolved Bugs: Added resolved bugs list for BSF release 22.3.2.

Release 2.22.3 - F69946-13, October 2022

Updated the following section with the details of UDR ATS 22.3.3 Release:

- UDR Resolved Bugs: Updated to add resolved bug list for UDR ATS release 22.3.3.

Release 2.22.3 - F69946-12, October 2022

Updated the following sections with the details of SCP 22.3.1, BSF 22.3.2, and Policy 22.3.2 Releases:

- Media Pack: Updated the media pack details.
- Compliance Matrix: Updated the compliance matrix information.
- Common Microservices Load Lineup: Updated the common services load lineup details.
- Security Certification Declaration : Added security declaration.
- Service Communication Proxy (SCP): Added the feature details for SCP release 22.3.1.
- SCP Resolved Bugs: Added resolved bugs list for SCP release 22.3.1.
- SCP Known Bugs: Added known bugs list for SCP release 22.3.1.
- Binding Support Function (BSF): Added the feature details for BSF release 22.3.2.
- BSF Resolved Bugs: Added resolved bugs list for BSF release 22.3.2.
- BSF Known Bugs: Added known bugs list for BSF release 22.3.2.
- Cloud Native Core Policy (CNC Policy): Added the feature details for CNC Policy release 22.3.2.
- CNC Policy Resolved Bugs: Added resolved bugs list for CNC Policy release 22.3.2.
- CNC Policy Known Bugs: Added known bugs list for CNC Policy release 22.3.2.

Release 2.22.3 - F69946-11, October 2022

Updated the following sections with the details of CNC Console 22.3.1, cnDBTier 22.3.1, NRF 22.3.1, and UDR 22.3.3 Releases:

- Media Pack: Updated the media pack details.
- Compliance Matrix: Updated the compliance matrix information.
- Common Microservices Load Lineup: Updated the common services load lineup details.
- Security Certification Declaration : Added security declaration.
- Cloud Native Core Console (CNC Console): Added the feature details for CNC Console release 22.3.1.

- CNC Console Resolved Bugs: Added resolved bugs list for CNC Console release 22.3.1.
- DBTier Resolved Bugs: Added resolved bugs list for cnDBTier release 22.3.1.
- Network Repository Function (NRF): Added the feature details for NRF release 22.3.1.
- NRF Resolved Bugs: Added resolved bugs list for NRF release 22.3.1.
- Unified Data Repository (UDR): Added the feature details for UDR release 22.3.3.
- UDR Resolved Bugs: Added resolved bugs list for UDR release 22.3.3.
- UDR Known Bugs: Added known bugs list for UDR release 22.3.3.

Release 2.22.3 - F69946-10, October 2022

Updated the following sections with the details of CNE 22.3.1, NEF 22.3.1, NSSF 22.3.1, SEPP 22.3.1, and CDCS 22.3.1 Releases:

- Media Pack: Updated the media pack details.
- Compliance Matrix: Updated the compliance matrix information.
- Common Microservices Load Lineup: Updated the common services load lineup details.
- Security Certification Declaration : Added security declaration.
- Network Exposure Function (NEF): Added the feature details for NEF release 22.3.1.
- CNE Resolved Bugs: Added resolved bugs list for CNE release 22.3.1.
- DBTier Resolved Bugs: Added resolved bugs list for DBTier release 22.3.1.
- NSSF Resolved Bugs: Added resolved bugs list for NSSF release 22.3.1.
- SEPP Resolved Bugs: Added resolved bugs list for SEPP release 22.3.1.
- SEPP Known Bugs: Added known bugs list for SEPP release 22.3.1.

Release 2.22.3 - F69946-08, September 2022

Updated the following sections with the details of CNE 22.3.1 and OSO 22.3.1 Releases:

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

Release 2.22.3 - F69946-07, September 2022

Updated the following sections with the details of UDR 22.3.1 and 22.3.2 Releases:

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

Release 2.22.3 - F69946-06, September 2022

Updated the document with the details of CNC Policy 22.3.1 Release:

- Added the list of CNC Policy 22.3.1 features to Cloud Native Core Policy (CNC Policy).
- Updated the following sections with the details of CNC Policy 22.3.1:
  - Media Pack
  - Compliance Matrix
  - Common Microservices Load Lineup
  - Security Certification Declaration
  - CNC Policy Resolved Bugs
  - CNC Policy Known Bugs

Release 2.22.3 - F69946-05, September 2022

Cosmetic updates

Release 2.22.3 - F69946-04, September 2022

NWDAF Release 22.0.0
Updated the document with the details of NWDAF 22.0.0 Release:

- Networks Data Analytics Function (NWDAF): Added the feature details for NWDAF release 22.0.0.
- Media Pack: Added the media pack details for NWDAF release 22.0.0.
- Compliance Matrix: Added the compliance matrix information for NWDAF release 22.0.0.
- Common Microservices Load Lineup: Added the common services load lineup details for NWDAF release 22.0.0.
- Security Certification Declaration : Added security declaration for NWDAF release 22.0.0.
- NWDAF Resolved Bugs: Added resolved bugs list for NWDAF release 22.0.0.
- NWDAF Known Bugs: Added known bugs list for NWDAF release 22.0.0.

Release 2.22.3 - F69946-03, September 2022

BSF Release 22.3.0
Updated the document with the details of BSF 22.3.0 Release:

- Binding Support Function (BSF): Added the feature details for BSF release 22.3.0.
- Media Pack: Updated the media pack details for BSF release 22.3.0.
- Compliance Matrix: Updated the compliance matrix information for BSF release 22.3.0.
- Common Microservices Load Lineup: Updated the common services load lineup details for BSF release 22.3.0.
- Security Certification Declaration : Added security declaration for BSF release 22.3.0.

- BSF Resolved Bugs: Added resolved bugs list for BSF release 22.3.0.
- BSF Known Bugs: Added known bugs list for BSF release 22.3.0.

CNC Policy Release 22.3.0
Updated the document with the details of CNC Policy 22.3.0 Release:

- Cloud Native Core Policy (CNC Policy): Added the feature details for CNC Policy release 22.3.0.
- Media Pack: Updated the media pack details for CNC Policy release 22.3.0.
- Compliance Matrix: Updated the compliance matrix information for CNC Policy release 22.3.0.
- Common Microservices Load Lineup: Updated the common services load lineup details for CNC Policy release 22.3.0.
- Security Certification Declaration : Added security declaration for CNC Policy release 22.3.0.
- CNC Policy Resolved Bugs: Added resolved bugs list for CNC Policy release 22.3.0.
- CNC Policy Known Bugs: Added known bugs list for CNC Policy release 22.3.0.

NRF Release 22.3.0
Updated the document with the details of NRF 22.3.0 Release:

- Network Repository Function (NRF): Added the feature details for NRF release 22.3.0.
- Media Pack: Updated the media pack details for NRF release 22.3.0.
- Compliance Matrix: Updated the compliance matrix information for NRF release 22.3.0.
- Common Microservices Load Lineup: Updated the common services load lineup details for NRF release 22.3.0.
- Security Certification Declaration : Added security declaration for NRF release 22.3.0.
- NRF Resolved Bugs: Added resolved bugs list for NRF release 22.3.0.
- NRF Known Bugs: Added known bugs list for NRF release 22.3.0.

Release 2.22.3 - F69946-02, September 2022

Removed the OSO details of SEPP Release 22.3.0 from the Compliance Matrix section.

Release 2.22.3 - F69946-01, August 2022

This is an initial release of this document for Release 2.22.3.

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 2.22.3.

2.1 Automated Testing Suite (ATS) Framework

Oracle Communications Cloud Native Core Automated Test Suite (ATS) framework 22.3.x has been updated with the following enhancements:

Release 22.3.1

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

Release 22.3.0

Oracle Communications Cloud Native Core Automated Test Suite (ATS) framework 22.3.0 has been updated with the following enhancements:

- **ATS Maintenance Scripts**: ATS Maintenance Scripts are used to take a backup of the ATS custom folders and Jenkins pipeline, view the configuration and restore the Jenkins pipeline, and install or uninstall ATS and Stubs. For more information, see *Oracle Communications Cloud Native Core Automated Testing Suite Guide.*

2.2 Binding Support Function (BSF)

Release 22.3.4

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

Release 22.3.2

Oracle Communications Cloud Native Core Binding Support Function (BSF) 22.3.2 has been updated with the following enhancements:

- **Enable Controlled Shutdown of an Instance:** CNC BSF supports controlled shutdown feature to provide the partial or complete isolation of the site from the network so that the operator can perform necessary recovery procedures when required. For more information on this feature and its configurations, see the "Enable controlled shut down of an instance" section in *Oracle Communications Cloud Native Core Binding Support Function User Guide*.
- **Enhancements to Aspen Service Mesh (ASM) Sidecar configuration:** The ASM Sidecar configuration is enhanced with the addition of Authorization Policy (AP) and Virtual Service (VS) CRDs to the Data Plane. The Service Mesh Authorization Policies at the ingress side-car associated with a server are used to filter requests originating from the clients using one of the identifiers (SPIFFE, FQDN or NF-type) contained within the client certificate. For more details, see the, "Aspen Service Mesh Configurations" section in *Oracle Communications Cloud Native Core Binding Support Function User Guide*.

Release 22.3.0

Oracle Communications Cloud Native Core Binding Support Function (BSF) 22.3.0 has been updated with the following enhancements:

- **Active Session Counter:** BSF facilitates counting the number of active sessions for a configurable time period. Also, it enables displaying the number of active sessions at any given time. For more information on this feature and its configurations, see the "Support for Active Sessions Counter" section in *Oracle Communications Cloud Native Core Binding Support Function User Guide*.
- **Support for User-Agent Header:** BSF supports the user-agent header, which helps the producer Network Function (NF) to identify the consumer NF that has sent the request. For more information on this feature and its configurations, see the "Support for User-Agent Header" section in *Oracle Communications Cloud Native Core Binding Support Function User Guide*.

2.3 Continuous Delivery Control Server (CDCS)

Oracle Communications Cloud Native Core Continuous Delivery Control Server (CDCS) 22.3.x has been updated with the following enhancements:

CDCS Release 22.3.1

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

CDCS Release 22.3.0

Oracle Communications Cloud Native Core Continuous Delivery Control Server (CDCS) 22.3.0 has been updated with the following enhancements:

- **Support for a Staging Site**: CDCS supports staging sites that are non-production sites where customers can install or upgrade NFs without affecting production traffic. For more information about the staging sites, see the "Managing Staging Sites" section in *Oracle Communications Cloud Native Core CD Control Server User Guide*.
- **Support for ATS Tests**: Automated test suites (ATS) are provided by each NF as a way to perform automated testing for each NF. Depending on the NF, the following automated tests may be provided:
  - Feature tests
  - Regression tests
  - Performance tests

  In this release, CDCS adds the ability to run ATS tests. Each NF releases an ATS CSAR with each release. ATS CSARs must be downloaded to CDCS, and installed at a Staging Site. Additionally, the NF CSAR itself must be downloaded and installed at the same Staging Site before the ATS tests can be run. For more information about the testing NF ATS, see the "Testing NFs" section in *Oracle Communications Cloud Native Core CD Control Server User Guide*.
- **Support for NF Uninstallation**: CDCS adds the ability to uninstall any NF that has been installed by CDCS, or has otherwise been identified through the Update NF Inventory command. For more information about uninstalling NF, see the "Uninstalling NF" section in *Oracle Communications Cloud Native Core CD Control Server User Guide*.

- **Support for Sending Email notification:** CDCS sends an email notification to configured email addresses when any command is run on CDCS. For more information about configuring an email, see the "Adding Email Address to Notification List" section in *Oracle Communications Cloud Native Core CD Control Server User Guide*.
- **Signed Artifact Verification**: CDCS supports verifying cryptographically signed artifacts in CSARs. As NF releases include these signed artifacts in their CSARs, CDCS will automatically perform signature verification when the CSAR is downloaded. NF CSARs that only provide checksums can still be downloaded, but only checksum verification will be performed. For more information about verifying the artifact, see the "Installing CDCS" section in *Oracle Communications Cloud Native Core CD Control Server Installation and Upgrade Guide*.

CD Control Server is compatible with the following NF versions:

- CNC Console 22.3.0
- cnDBTier 22.3.0
- SCP 22.3.0
- SEPP 22.3.0

2.4 Cloud Native Core Console (CNC Console)

Oracle Communications Cloud Native Core Console (CNC Console) 22.3.x has been updated with the following enhancement.

Release 22.3.2

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

Release 22.3.1

Oracle Communications Cloud Native Core Console (CNC Console) 22.3.1 has been updated with the following enhancement:

- **Added new API prefix at Console for EIR mode in UDR/SLF**: To enable the EIR mode of UDR in CNC Console, new API prefix is introduced in CNC Console. For information about EIR Prefix, see the "*CNC Console KPIs*" and "*CNC Console Metrics*" sections in *Oracle Communications Cloud Native Core User Guide*.

Release 22.3.0

Oracle Communications Cloud Native Core Console (CNC Console) 22.3.0 has been updated with the following enhancement:

- **Support for CNC Console Deployment using Continuous Delivery Control Server (CDCS):** In addition to CNC Console's Command Line Interface (CLI) deployment method, CNC Console can be deployed using the Continuous Delivery Control Server (CDCS), which is a centralized server that automates CNC Console deployment processes such as downloading the CNC Console package, installation, upgrade, and rollback. For more information about CDCS, see *Oracle Communications Cloud Native Core CD Control Server User Guide*. For information about CNC Console deployment using CDCS, see the "Overview" section in *Oracle Communications Cloud Native Core Console Installation and Upgrade Guide*.
- **Supports Single Helm chart for CNC Console Deployment**: Until the current release, CNC Console was using two helm charts to deploy CNCC IAM and M-CNCC Core or A-CNCC Core components. With this feature, CNC Console will be able to deploy all the

components as part of a single helm chart deployment. For more information about the Single Helm chart for CNC Console Deployment, see *Oracle Communications Cloud Native Core Console Installation and Upgrade Guide*.

- **Compliance with ASM 1.9.x and Kubernetes 1.20**: CNC Console deployment has been enhanced to be in compliance with ASM 1.9.x and Kubernetes 1.20. For more information, see Oracle Communications Cloud Native Core Console Installation and Upgrade Guide.
- **Supports the Latest Version of NFs**: CNC Console is compatible with the following NF versions:
  - SCP 22.3.0
  - NRF 22.3.0
  - UDR 22.3.0
  - SEPP 22.3.0
  - NSSF 22.3.0
  - BSF 22.3.0
  - POLICY 22.3.0

  For more information, see the "CNC Console Deployment Modes" section in *Oracle Communications Cloud Native Core Console Installation and Upgrade Guide* and *Oracle Communications Cloud Native Core Console User Guide*.

2.5 Cloud Native Core DBTier (cnDBTier)

Oracle Communications Cloud Native Core DBTier (cnDBTier) 22.3.x has been updated with the following enhancements:

Release 22.3.4

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

Release 22.3.3

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

Release 22.3.2

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

Release 22.3.1

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

Release 22.3.0

Oracle Communications Cloud Native Core DBTier (cnDBTier) 22.3.0 has been updated with the following enhancements:

- **DBTier Scaling**: DBTier supports horizontal and vertical scaling of MySQL Application PODs for improved performance. For more information about the feature, see "DBTier Scaling" in *Oracle Communications Cloud Native Core DBTier User Guide*.

- **DBTier Support for Multi Channel Georeplication**: DBTier supports multichannel georeplication feature that improves the georeplication performance between sites by replicating multiple databases parallelly. As a part of this feature, the DBTier site addition procedure has been updated to support multichannel georeplication feature. This feature also introduces the procedure to convert a single replication channel group to multiple channel replication group. For more information about the feature, see *Oracle Communications Cloud Native Core DBTier User Guide*.
- **DBTier Rollback Procedure**: DBTier supports rollback from DBTier version 22.3.x to release 22.2.x and release 22.1.x. For more information on the rollback procedures, see *Oracle Communications Cloud Native Core DBTier Disaster Recovery Guide*.
- **TLS Security Scan:** Manual procedure to run TLS Security has been introduced in this release. This procedure will be integrated in the CI/CD pipeline in the next release.
- **New Versions of MySQL Cluster Software:** Oracle MySQL Cluster Database - 8.0.30 software is upgraded in this release.

2.6 Cloud Native Environment (CNE)

Oracle Communications Cloud Native Environment (OCCNE) 22.3.x has been updated with the following enhancements:

Release 22.3.3

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

Release 22.3.1

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

Release 22.3.0

Oracle Communications Cloud Native Environment (OCCNE) 22.3.0 has been updated with the following enhancements:

- **Virtual CNE Load Balancer Support for TLS**: 5G Network Functions use TLS to encrypt communications between themselves. However, until the current release, the load balancers used in virtualized OCCNE deployments were not supporting TLS and blocked the TCP and HTTP connections. Now, OCCNE load balancers support TLS-encrypted protocols, such as HTTPS. This enables the load balancers to establish and manage TLS on TCP and HTTP connections.
- **Enhanced Virtual CNE Load Balancer Switchover Performance**: In case of an Active Load Balancer VM (LBVM) failure, the system took excessive time to switchover between an active and standby Load balancer. Now, the LBVM switchover time has been considerably improved. In most cases, the switchover time is reduced by at least 75%.
- **Bastion Host Liveness Alerts**: New alerting rules have been defined in OCCNE to raise alerts when a Bastion Host becomes unavailable. For more information on these alerts, see Oracle Communication Cloud Native Environment User Guide.
- **Supports New Version of Common Services**: CNE is now compatible with the following common services versions:
  - Helm - 3.8.2
  - Kubernetes - 1.23.7
  - containerd - 1.6.4

- Calico - 3.22.3
- MetalLB - 0.12.1
- Prometheus - 2.36.1
- Grafana - 7.5.11
- Jaeger - 1.28.0
- Istio - 1.13.2
- cert-manager - 1.6.2

Operation Service Overlays (OSO)

Operation Service Overlays (OSO) 22.3.x has been updated with the following enhancements:

Release 22.3.2
Operation Service Overlays (OSO) 22.3.2 has been updated with the following enhancements:

- **New Versions of Services**: The following services are upgraded in this release:
  - Prometheus - 2.39.1
  - configmap-reload - 0.8.0

Release 22.3.1
Operation Service Overlays (OSO) 22.3.1 has been updated with the following enhancements:

- **New Versions of Services**: The following services are upgraded in this release:
  - NGINX Ingress Controller - 1.3.1
  - configmap-reload - 0.7.0

Release 22.3.0
Operation Service Overlays (OSO) 22.3.0 has been updated with the following enhancements:

- **Restoration of OSO non-HA Prometheus version**: The previous version of OSO used Prometheus Operator to implement HA Prometheus (High Availability Prometheus). Prometheus Operator requires the creation of CRD definitions to operate. The customers were unable to create CRD definitions as ClusterRole permissions are required to create CRD definitions. To overcome these restrictions, OSO 22.3.0 has excluded Prometheus Operator and has restored the non-HA Prometheus version. For information on OSO installation, see *Oracle Communications Operations Services Overlay (OSO) Installation Guide*.
- **New Versions of Services**: The following services are upgraded in this release:
  - Prometheus - 2.36.1
  - Grafana - 7.5.11

2.7 Cloud Native Core Policy (CNC Policy)

Release 22.3.4

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

Release 22.3.3

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

Release 22.3.2

Oracle Communications Cloud Native Core Policy 22.3.2 has been updated with the following enhancements:

- **Subscriber Tracing Support for AM Policy Service**: CNC PCF supports subscriber tracing for AM policy that allows defining a list of subscribers that you may require to troubleshoot the NFs and trace the logs. For more details, see the "Subscriber Activity Logging" section in *Oracle Communications Cloud Native Core Policy User Guide*.
- **Subscriber Tracing Support for UE Policy Service**: CNC PCF supports subscriber tracing for UE policy that allows defining a list of subscribers that you may require to troubleshoot the NFs and trace the logs. For more details, see the "Subscriber Activity Logging" section in *Oracle Communications Cloud Native Core Policy User Guide*.
- **Handling Stale Data in PDS for AM Service and UE Policy Service**: This feature leverages the resetContext and revalidation functionalities in PDS to handle the stale PDS subscriber data when there are multiple sessions for AM Service or UE Policy Service. For more details, see "Handling Stale Data in PDS" section in *Oracle Communications Cloud Native Core Policy User Guide*.
- **Limiting the Number of Sessions for AM Service and UE Policy Service**: This feature enables to configure the Max Session Limit Per User for a subscriber when Enable Max Session Limit flag is enabled for a policy service. This avoids duplicate and stale data in the respective policy service databases (such as AMPolicyAssociations and UEPolicyAssociations). For more details, see "Limiting the Number of Sessions" section in *Oracle Communications Cloud Native Core Policy User Guide*.
- **Stale Session Detection and Handling in UE Service**: The Existing stale session detection and handling functionality in CNC Policy is enhanced to identify and remove the stale sessions for UE Policy Service. A UE Policy Association on PCF is considered as stale when the association exists in PCF, but has no corresponding session on the AMF. When a UE Policy Association is detected as stale, the UE Policy Service deletes the association from the database. For more details on Stale Session Detection and Handling in UE Service, see "Stale Session Handling" section in *Oracle Communications Cloud Native Core Policy User Guide*.
- **Support for MSISDN/GPSI lookup Key to Fetch N36 (Nudr) Record**: CNC Policy supports MSISDN or GPSI as N36 key. For more information, see "PCF User Connector" section in *Oracle Communications Cloud Native Core Policy User Guide*.

Release 22.3.1

Oracle Communications Cloud Native Core Policy 22.3.1 has been updated with the following enhancements:

- **Enhancements to Aspen Service Mesh (ASM) Sidecar configuration**: The ASM Sidecar configuration is enhanced with the addition of Authorization Policy (AP) and Virtual Service (VS) CRDs to the Data Plane. The Service Mesh Authorization Policies at the ingress side-car associated with a server are used to filter requests originating from the clients using one of the identifiers (SPIFFE, FQDN or NF-type) contained within the client certificate.
  For more details, see the "Aspen Service Mesh Configurations" section in *Oracle Communications Cloud Native Core Policy Installation Guide*.

- **Support for enabling or disabling controlled shutdown feature**: CNC Policy supports enabling or disabling controlled shutdown feature. To enable the feature, set the value of *enableControlledShutdown* flag to *true* in the custom.yaml file. For more details, see the "Controlled Shutdown Configuration" section in *Oracle Communications Cloud Native Core Policy Installation Guide*.

Release 22.3.0

Oracle Communications Cloud Native Core Policy 22.3.0 has been updated with the following enhancements:

- **Subscription to Notification Support for Signaling Path Status:** CNC Policy supports notification, subscription to notification, and cancellation of the subscription to notification for signaling path status. For more information on this feature and its configurations, see the "Subscription to Notification Support for Signaling Path Status" section in *Oracle Communications Cloud Native Core Policy User Guide*.
- **Enable Controlled Shutdown of an Instance:** CNC Policy supports controlled shutdown feature to provide the partial or complete isolation of the site from the network so that the operator can perform necessary recovery procedures when required. For more information on this feature and its configurations, see the "Enable controlled shut down of an instance" section in *Oracle Communications Cloud Native Core Policy User Guide*.
- **Support for SessionRuleErrorHandling:** CNC Policy supports SessionRuleErrorHandling which helps in deciding whether to retain the old session rule, re-install, modify, or remove the session rule. For more information on this feature and its configurations, see the "Support for SessionRuleErrorHandling" section in *Oracle Communications Cloud Native Core Policy User Guide*.
- **Optimizing Policy Table:** Policy table has been enhanced and optimized to have more tables, rows, and columns for the services. For more information on this feature and its configurations, see the "Policy Table" section in *Oracle Communications Cloud Native Core Policy User Guide*.
- **Support for local configuration of UDR, CHF, NF profile:** CNC Policy has implemented new APIs which allow the users to configure UDR/CHF/AMF/BSF NF profile through CM Service API. For more information on this feature and its configurations, see the "NF Profile" section in *Oracle Communications Cloud Native Core Policy REST API Guide*.
- **Convert PCRF-Core to SpringBoot:** The Cloud native PCRF-Core application has been converted from Java to SpringBoot application. For more information on PCRF Core Metrics, see the "PCRF Core Metrics" section in *Oracle Communications Cloud Native Core Policy User Guide*.
- **Support for Retrying Binding Registration on BSF and generating Alarm to Operator:** CNC Policy supports the enhanced binding registration functionality between SM Service and BSF with the Retry Binding Registration on BSF feature. It retries BSF registrations until a maximum number of attempts are reached or the response error code does not match with any of the configured error codes. For more information on this feature and its configurations, see the "Support for Retrying Binding Registration on BSF and generating Alarm to Operator" section in *Oracle Communications Cloud Native Core Policy User Guide*.
- **Enhancement to use Cached NRF Discovery Responses:** Starting with release 22.3.0, PCF is enhanced to maintain a cache of the NF Profiles discovered

through the NRF discovery with their query parameters. This functionality enables PCF to use the cached NRF discovery responses in case of NRF discovery failure and expired or suspended NF producers. CNC Policy provides an option to configure the cache per interface,with the default value astrue**.** For more information on this feature and its configurations, see the "Support for Cached NRF Discovery Responses" section in *Oracle Communications Cloud Native Core Policy User Guide*.

- **Support for Sd Interface:** CNC Policy supports the Sd interface that enables it to communicate with the Traffic Detection Function (TDF). The Sd interface allows provisioning of the Application Detection and Control (ADC) rules from CNC Policy for traffic detection and enforcement at the TDF through Solicited Application Reporting. For more information on this feature and its configurations, see the "Support for Sd Interface" section in *Oracle Communications Cloud Native Core Policy User Guide*.
- **Support for Concurrency Handling using Bulwark Service:** CNC Policy supports the Bulwark service to handle the concurrent requests coming from other Policy services. The Bulwark service integrates with the SM service to handle the concurrent requests for the SM Create and Delete procedures. The SM service integration with Bulwark service handles the concurrent requests for the same subscriber in a concurrent and efficient manner. For more information on this feature and its configurations, see the "Support for Concurrency Handling using Bulwark Service" section in *Oracle Communications Cloud Native Core Policy User Guide*.
- **Audit support for Binding service:** CNC Policy supports the Audit configurations for the Binding service. For more information about the enhanced configuration, see the "Configuring CNC Policy Using CNC Console" section in *Oracle Communications Cloud Native Core Policy User Guide*.
- **Enhanced Session Viewer User Interface:** The Session Viewer user interface in CNC Console for Policy has been enhanced better user experience. For more information, see the "Configuring CNC Policy Using CNC Console" section in *Oracle Communications Cloud Native Core Policy User Guide*.
- **Perf-Info Capacity Configuration:** CNC Policy allows you to configure the capacity for the perf-info service using the Custom Values YAML file during the installation. For more information about the configurations, see the "Customizing CNC Policy" section in *Oracle Communications Cloud Native Core Policy User Guide*.
- **Enhanced PRE Logs for Policy Table Evaluation:** CNC Policy provides enhanced troubleshooting by including table name, column name, and row value in the PRE Logs instead of the Hex ID of the table, column, and row. For more information about the configurations, see the "Logs" section in *Oracle Communications Cloud Native Core Policy Troubleshooting Guide*.

2.8 Network Exposure Function (NEF)

Oracle Communications Cloud Native Core Network Exposure Function (NEF) 22.3.x has been updated with the following enhancements:

Release 22.3.2

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

Release 22.3.1

Oracle Communications Cloud Native Core Network Exposure Function (NEF) 22.3.1 has been updated with the following enhancement:

- **Support for Update AF Session with QoS**: The OCNEF QoS (Quality of Service) is enhanced to support the PUT and PATCH operations that enable the operators to modify existing QoS subscriptions. For more information about the feature, see the "Support for AF Session with QoS"section in *Oracle Communications Cloud Native Core Network Exposure Function User Guide*.

Release 22.3.0

Oracle Communications Cloud Native Core Network Exposure Function (NEF) 22.3.0 has been updated with the following enhancements:

- **Support for AF Session with ASQoS**: The OCNEF architecture is enhanced to support the QoS (Quality of Service) service that enables the operators to provide quality-related specifications to the 5G Network Functions (NFs). The NFs process the provisioned data to support the services as specified by the operators and send notifications. For more information about the feature, see "Support for AF Session with AsQoS" in *Oracle Communications Cloud Native Core Network Exposure Function User Guide*.
- **Support for Distributed Architecture**: The OCNEF architecture allows the operators to install OCNEF and OCCAPIF components in separate Kubernetes namespaces. For more information about the architecture, see the "OCNEF Architecture" in the *Oracle Communications Cloud Native Core Network Exposure Function User Guide*.

2.9 Network Repository Function (NRF)

Oracle Communications Cloud Native Core Network Repository Functions (NRF) 22.3.x has been updated with the following enhancements.

OCNRF Release 22.3.2

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

OCNRF Release 22.3.1

Oracle Communications Cloud Native Core Network Repository Functions (NRF) 22.3.1 has been updated with the following enhancement:

- **Support for Parameterization in NRF-ATS**: With this feature NRF-ATS GUI has an option to either run the test cases with default product configuration or with custom configuration. You can provide values for the input and output parameters needed for the test cases to be compatible with SUT configuration. You can update the key-value pair values in the `global.yaml` and `feature.yaml` files for each of the feature files so that it is compatible with SUT configuration. For more information about the feature, see the "NRF-NewFeatures Pipeline" section in *Oracle Communications Cloud Native Core Automated Testing Suite Guide*.

OCNRF Release 22.3.0

Oracle Communications Cloud Native Core Network Repository Functions (NRF) 22.3.0 has been updated with the following enhancements:

- **Support for four-site Georedundancy**: OCNRF is enhanced to support four-sites Geographical Redundant (Georedundant) deployment. It offers, four-sites, three-sites, and two-sites georedundancy to ensure service availability when one of the OCNRF sites is down. For more information about the feature, see the "OCNRF

Georedundacy" section in *Oracle Communications Cloud Native Core Network Repository Function User Guide*.

- **Support for Notification Retries**: OCNRF supports notification retry mechanism in case of failures in sending Notification message. Based on the configured Notification Retry Profile, the OCNRF attempts to re-send the Notification message on failures until the retry attempt is exhausted. For more information about the feature, see "Notification Retry" section in *Oracle Communications Cloud Native Core Network Repository Function User Guide*.
- **Support for HA and PDB for NRF Auditor POD**: OCNRF supports two pods of Auditor microservice to provide High Availability (HA) and PodDisruptionBudget (PDB) functionality. For more information about the feature and the list of services supporting HA and PDP, see "PodDisruptionBudget Kubernetes Resource" section in *Oracle Communications Cloud Native Core Network Repository Function Installation and Upgrade Guide*.
- **Support for R16 NFs CBCF and NSSAAF**: OCNRF supports the following 3GPP TS 29.510 Release 16 nfTypes:
  - Network Slice Specific Authentication and Authorization Function (NSSAAF)
  - Cell Broadcast Center Function (CBCF)
  - Mobility Management Entity (MME)
  - Interrogating Call Session Control Function (ICSCF)
  - Security Assurance Specification (SCSAS)
  - Diameter Routing Agent (DRA)
  - UE Capability Management Function (UCMF)
  - Steering of Roaming Application Function (SOR_AF)
  - Secured Packet Application Function (SPAF)
  - Service Capability Exposure Function (SCEF)
  - IP Multimedia Subsystem Application Server (IMS_AS)

  For more information about the nfTypes, see "Supported NF Types" section in *Oracle Communications Cloud Native Core Network Repository Function User Guide*.
- **Support for NRF Access Policies to Restrict Ingress and Egress Traffic**: OCNRF provides network access policies to enforce access restrictions for all the applicable data flows except communication from Kubernetes node to pod for invoking container probe. For more information about configuring the network policies, see the "Configuring Network Policies" section in *Oracle Communications Cloud Native Core Network Repository Function Installation and Upgrade Guide*.

2.10 Network Slice Selection Function (NSSF)

Oracle Communications Network Slice Selection Function (NSSF) 22.3.x has been updated with the following enhancements:

NSSF Release 22.3.2

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

NSSF Release 22.3.1

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

NSSF Release 22.3.0

Oracle Communications Network Slice Selection Function (NSSF) 22.3.0 has been updated with the following enhancements:

- **Support for Autopopulation of Configuration Based on NsAvailability Update**: Currently, the data received from Nnssf_NSSAIAvailability update is not replicated to the provisional configuration (site-specific database). However, the data are crucial, as they are used in Nnssf_NSSelection service's operations. The operator is required to configure not only the allowed S-NSSAI information from the AMF but also the restricted S-NSSAIs per TAC per PLMN. After this enhancement, the operator need not configure the allowed S-NSSAIs. It will be updated automatically based on the NsAvailability update from the AMF. The operator is required to configure only the restricted S-NSSAI information per TAC per PLMN. For more information, see "Autopopulation of Configuration Based on NsAvailability Update" in *Oracle Communications Cloud Native Core Network Slice Selection Function User Guide.*
- **Handover from EPS to 5G**: This feature allows slice allocation to subscribers when they move from 4G to 5G network. For more information, see "Handover from EPS to 5G" in *Oracle Communications Cloud Native Core Network Slice Selection Function User Guide.*

2.11 Networks Data Analytics Function (NWDAF)

OCNWDAF Release 22.0.0

This is the first release of Oracle Communications Network Data Analytics Functions (OCNWDAF).

OCNWDAF provides the following features:

- **Data collection from AMF, SMF, and NRF**: OCNWDAF interacts with 5G NFs over the Service Based Interface (SBI) directly or through NEF for the data collection. For more information about the data collection by OCNWDAF, see "OCNWDAF Interfaces" section in *Oracle Communications Networks Data Analytics Function User Guide*.
- **Analytics Generation**: OCNWDAF generates various kind of analytics reports for providing analytics information to the consumer NFs. It supports the following types of analytics information:
  - Slice Load level information
  - UE Mobility information
  - UE Abnormal Behavior information (Unexpected UE location)

  For more information about each type of analytics, see the "OCNWDAF Analytics" section in *Oracle Communications Networks Data Analytics Function User Guide*.

2.12 Service Communication Proxy (SCP)

Oracle Communications Cloud Native Core Service Communication Proxy (SCP) 22.3.x has been updated with the following enhancements.

Release 22.3.4

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

Release 22.3.3

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

Release 22.3.2

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

Release 22.3.1

Oracle Communications Cloud Native Core Service Communication Proxy (SCP) 22.3.1 has been updated with the following enhancements:

- **SCP Observability Enhancement**: SCP adds the "User-Agent" header to the SCP originated message requests to NRF. The format of the "User-Agent" header is defined using the `userAgentHeaderFormat` REST API parameter. This enhancement enables SCP to support User-Agent formats and includes consumer NFs identity as dimensions in SCP metrics, alerts, and logs. The following dimensions are introduced as part of this enhancement to filter SCP metrics based on the consumer NF information: ocscp_consumer_host, ocscp_consumer_nf_instance_id, and ocscp_consumer_nf_type. For more information, see "5G SBI Message Routing" in *Oracle Communications Cloud Native Core Service Communication Proxy User Guide*.
- **Compliance with ASM 1.11.8 and Kubernetes 1.23.x**: SCP deployment has been enhanced to be in compliance with ASM 1.11.8 and Kubernetes 1.23.x. For more information, see *Oracle Communications Cloud Native Core Service Communication Proxy Installation and Upgrade Guide*.

Release 22.3.0

Oracle Communications Cloud Native Core Service Communication Proxy (SCP) 22.3.0 has been updated with the following enhancements:

- **Enhanced NF Status Processing:** The existing Network Function (NF) Status Processing feature is enhanced to enable SCP to route 5G Service Based Interface (SBI) message requests to the SUSPENDED target producer NF if the REGISTERED alternate producer NFs are unavailable or respond with an error code that qualifies for rerouting. For more information, see "Enhanced NF Status Processing" in *Oracle Communications Cloud Native Core Service Communication Proxy User Guide*.
- **Ingress Rate Limiting Using the User-Agent Header**: The existing Ingress Rate Limiting feature is enhanced to enable SCP to use the User-Agent or XFCC header in the ingress message request to identify the consumer NF and apply ingress rate limiting at the ingress side. For more information, see "Ingress Rate Limiting" in *Oracle Communications Cloud Native Core Service Communication Proxy User Guide*.

2.13 Security Edge Protection Proxy (SEPP)

Oracle Communications Cloud Native Core Security Edge Protection Proxy (SEPP) 22.3.x has been updated with the following enhancements:

SEPP Release 22.3.2

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

SEPP Release 22.3.1

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

SEPP Release 22.3.0

Oracle Communications Cloud Native Core Security Edge Protection Proxy (SEPP) 22.3.0 has been updated with the following enhancements:

- **SBI Message Mediation Support**: The 5G SBI Message Mediation Support feature at SEPP allows Mobile Network Operators (MNO)s to resolve the inter-op issues between PLMNs by manipulating the inter-PLMN messages. The SEPP must use the mediation service to support message mediation. The MNO shall rely on mediation service capabilities to provision the mediation rules. The SEPP shall support the following mediation trigger points to invoke mediation service:
  - Ingress inter-PLMN and core network messages
  - Egress inter-PLMN

  For more information about the feature, see the "5G SBI Message Mediation Support" section in *Oracle Communications Cloud Native Core Security Edge Protection Proxy User Guide* and the "Configuration Parameters" section in *Oracle Communications Cloud Native Core Security Edge Protection Proxy Installation and Upgrade Guide*.
- **Topology Hiding Phase 3**: SEPP provides message filtering and policing on inter-PLMN control plane interfaces and topology hiding. Topology hiding is a security feature in 5G that secures the address of the network elements and can prevent attacks intended for unauthorized access to network elements or interruption of the network service. The purpose of the feature is to enable topology hiding of information from the home or visited PLMN to the visited or Home PLMN. Topology hiding conceals identity information from all messages leaving a PLMN. Topology hiding Phase 3 supports the topology hiding of both body and header of the message. For more information about the feature,see the "Topology Hiding" section in *Oracle Communications Cloud Native Core Security Edge Protection Proxy User Guide* and the "Configuration Parameters" section in *Oracle Communications Cloud Native Core Security Edge Protection Proxy Installation and Upgrade Guide*.
- **Support of TLS for Roaming Hubs and IPX Providers**: Oracle SEPP is deployed by both Mobile Network Operators (MNO) and Internetwork Packet Exchange (IPX) providers. The roaming hub feature allows the user to deploy OCSEPP in either 5GC SEPP NF mode or Roaming Hub mode. For more information about the feature, see the "Support of TLS for Roaming Hubs and IPX Providers" section in *Oracle Communications Cloud Native Core Security Edge Protection Proxy User Guide* and the "Overview" section in *Oracle*

Communications Cloud Native Core Security Edge Protection Proxy Installation and Upgrade Guide.

- **Support for Upgrade and Rollback through CDCS**: In addition to SEPP's Command Line Interface (CLI) deployment method, SEPP can be deployed using the Continuous Delivery Control Server (CDCS), which is a centralized server that automates SEPP deployment processes of the upgrade and rollback. For more information about the feature, see the "Upgrading SEPP" section in *Oracle Communications Cloud Native Core Security Edge Protection Proxy Installation and Upgrade Guide*.
- **Overload control feature**: OCSEPP supports overload control to protect the pn32f-svc microservice from overload situations and maintain the overall health of the service. This feature helps you to protect, mitigate, and avoid entering into an overload condition, detect overload conditions, and take necessary actions to recover from overload on the basis of CPU and memory usage. N32 Ingress Gateway allows or discards incoming requests, based on the overload threshold applied or on the basis of SBI message priority. For more information about the feature, see the "Overload Control Feature" section in *Oracle Communications Cloud Native Core Security Edge Protection Proxy User Guide* and the "Configuration Parameters" section in *Oracle Communications Cloud Native Core Security Edge Protection Proxy Installation and Upgrade Guide*.
- **Global Rate Limiting on Egress Gateway of SEPP**: Global rate limiting feature is provided by Egress Gateway (plmn egress-gateway and n32-egress-gateway). With this feature, OCSEPP secures the network when aggregated egress traffic exceeds the allowed traffic rate limit. If the traffic exceeds the allowed traffic rate limit, OCSEPP does not process the traffic and responds with an error code. Egress global rate limiting the functionality of the OCSEPP allows the user to configure the acceptable egress traffic rate to any registered NF instance. For more information about the feature, see the "Global Rate Limiting on Egress Gateway of SEPP" section in *Oracle Communications Cloud Native Core Security Edge Protection Proxy User Guide* and the "Configuration Parameters" section in *Oracle Communications Cloud Native Core Security Edge Protection Proxy Installation and Upgrade Guide*.
- **Security Counter Measure Service API Validation feature**: There are certain 5G SBI messages which need not traverse networks (example: AMF and SMF interactions, NRF registration requests). The feature blocks these kinds of messages from traversing networks. The Security Counter Measure Service API Validation feature allows the operator to configure the allowed service APIs at the SEPP. The feature intends to support this in two ways:
  - Check the combination of METHOD and Service requested (Example: POST cannot be used in combination with a particular service).
  - Allows only certain SBI messages to either egress or ingress the network (Example: AMF to UDM messages). For more information about the feature,see the "Security Counter Measure Service API Validation" section in *Oracle Communications Cloud Native Core Security Edge Protection Proxy User Guide* and the "Configuration Parameters" section in *Oracle Communications Cloud Native Core Security Edge Protection Proxy Installation and Upgrade Guide*.
- **Helm Test**: Helm Test feature validates the installation of SEPP and determines if the Network Function (NF) is ready to accept traffic. For more information about the feature, see the "Performing Post installation Helm test" section and the "Configuration Parameters" section in *Oracle Communications Cloud Native Core Security Edge Protection Proxy Installation and Upgrade Guide*.
- **Helm Validation Framework**: The helm validation framework is added to validate the values in `custom_values.yaml` file with JSON schemas. If the `custom-values.yaml` file has some incorrect values or not the expected values, this framework

will catch the issues initially before starting the deployment or upgrade and display appropriate errors. Using this enhancement, the user can be sure that the deployment happened with the correct expected value. For more information about the feature, see the "Helm Validation Framework" section in *Oracle Communications Cloud Native Core Security Edge Protection Proxy User Guide* and the "Configuration Parameters" section in *Oracle Communications Cloud Native Core Security Edge Protection Proxy Installation and Upgrade Guide*.

- **Enhancement in Subject Alternate Name (SAN) Validation**: SAN (Subject Alternate Names) validates whether the SAN in the SEPP certificate matches with the sender FQDN received in the capability-exchange message. Previously (before SEPP Release 22.3.0), the SAN validation is a mandatory configuration for the regular SEPP deployments. With this enhancement, the SAN validation has become optional. The user now has the flexibility to either perform the validation on SAN or avoid validation as per the environment. For more information about the feature, see the "Enhancement in Subject Alternate Name (SAN) Validation" section in *Oracle Communications Cloud Native Core Security Edge Protection Proxy User Guide* and the "Configuration Parameters" section in *Oracle Communications Cloud Native Core Security Edge Protection Proxy Installation and Upgrade Guide*.

2.14 Unified Data Repository (UDR)

Oracle Communications Cloud Native Core Unified Data Repository (UDR) 22.3.x has been updated with the following enhancements:

Release 22.3.4

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

Release 22.3.3

Oracle Communications Cloud Native Core Unified Data Repository (UDR) 22.3.3 has been updated with the following enhancements:

- **Support for Subscriber Location Function (SLF) - Periodic Export of Subscriber Database:** This feature supports periodic exporting of SLF subscriber data into Comma Separated Value (CSV) file format using the Subscriber Export Tool. The Subscriber Export Tool is scheduled for daily runs and is deployed as a stand-alone tool. It also supports dynamic configuration of periodicity of export. For more information about the feature, see "Supports Periodic Export of SLF Subscriber Database", see *Oracle Communications Cloud Native Core Unified Data Repository User Guide*.

Release 22.3.2

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

Release 22.3.1

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

Release 22.3.0

Oracle Communications Cloud Native Core Unified Data Repository (UDR) 22.3.0 has been updated with the following enhancements:

- **Support for 5G EIR Signaling**: This feature introduces 5G Equipment Identity Register (EIR) functionality in the UDR. UDR will support a separate deployment mode for 5G EIR. For more information about the feature, see "Support for 5G EIR Signaling" in *Oracle Communications Cloud Native Core Unified Data Repository User Guide.* 5G EIR supports:
  - REST/JSON based provisioning of 5G EIR profile
  - Provisioning of 5G EIR entries via CNC Console or REST API
  - N5g-eir_EquipmentIdentityCheck Service API. N5g-eir is the service-based interface as defined by 3GPP
  - NRF registration of the EIR service
  - EIR Access Log for black and grey listed Permanent Equipment Identifier (PEI)
  - Bulk Import of 5G EIR subscriber data via PDBI interface
- **Support for 5G EIR Bulk Provisioning**: 5G EIR supports bulk provisioning of subscriber data via the batch files. This feature provides the capability of processing the batch files containing Eagle EPAP supported PDBI provisioning commands that enable deployment of 5G EIR in stand-alone mode. Bulk Import tool can be used to provision EIR subscribers using PDBI format. For more information about the feature, see "Support for 5G EIR Bulk Provisioning" and "Bulk Import Tool for EIR" in *Oracle Communications Cloud Native Core Unified Data Repository User Guide*.
- **Subscriber Activity Logging**: This feature enhances the logging functionality by UDR to support subscriber-specific logging. This enables the operators to log the subscriber activity for the configured list of subscribers. You can define a list of subscribers for which the logging is required, and this can be controlled irrespective of the log level that is enabled for UDR. You can collect the message exchanges, subscriber specific decision making, and logic handling for specific subscribers. For more information about the feature, see "Subscriber Activity Logging" in *Oracle Communications Cloud Native Core Unified Data Repository User Guide.*

3
Media and Documentation

3.1 Media Pack

This section lists the media package for Cloud Native Core 2.22.3. To download the media package, see MOS.

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

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

Table 3-1 Media Pack Contents for Cloud Native Core 2.22.3

Description	NF Version	ATS Version	Upgrade Supported
Oracle Communications Cloud Native Core Binding Support Function (BSF)	22.3.4	22.3.4	BSF 22.3.4 supports fresh installation and upgrade from 22.1.x, 22.2.x, and 22.3.0 to 22.3.4. For more information on installation or upgrade, see *Oracle Communications Cloud Native Core Binding Support Function Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core Binding Support Function (BSF)	22.3.2	22.3.1	BSF 22.3.2 supports fresh installation and upgrade from 22.1.x, 22.2.x, and 22.3.0 to 22.3.2. For more information on installation or upgrade, see *Oracle Communications Cloud Native Core Binding Support Function Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core Binding Support Function (BSF)	22.3.0	22.3.0	BSF 22.3.0 supports fresh installation and upgrade from 22.1.x and 22.2.x to 22.3.0. For more information on installation or upgrade, see *Oracle Communications Cloud Native Core Binding Support Function Installation and Upgrade Guide*.

Table 3-1 (Cont.) Media Pack Contents for Cloud Native Core 2.22.3

Description	NF Version	ATS Version	Upgrade Supported
Oracle Communications Cloud Native Core Console (CNC Console)	22.3.2	NA	CNC Console 22.3.2 supports fresh installation and upgrade from 22.1.x, 22.2.x , 22.3.x to 22.3.2. For more information on installation, see *Oracle Communications Cloud Native Core Console Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core Console (CNC Console)	22.3.1	NA	CNC Console 22.3.1 supports fresh installation and upgrade from 22.1.x, 22.2.x, 22.3.0 to 22.3.1. For more information on installation, see *Oracle Communications Cloud Native Core Console Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core Console (CNC Console)	22.3.0	NA	CNC Console 22.3.0 supports fresh installation and upgrade from 22.1.x, 22.2.x to 22.3.0. For more information on installation, see *Oracle Communications Cloud Native Core Console Installation and Upgrade Guide*.
Oracle Communications Cloud Native Environment (CNE)	22.3.3	NA	CNE 22.3.3 supports fresh installation and upgrade from 22.2.x, 22.3.x to 22.3.3. For more information on installation, see *Oracle Communications Cloud Native Environment Installation Guide*. For more information on upgrade, see *Oracle Communications Cloud Native Environment Upgrade Guide*.
Oracle Communications Cloud Native Environment (CNE)	22.3.1	NA	CNE 22.3.1 supports fresh installation and upgrade from 22.2.x, 22.3.0 to 22.3.1. For more information on installation, see *Oracle Communications Cloud Native Environment Installation Guide*. For more information on upgrade, see *Oracle Communications Cloud Native Environment Upgrade Guide*.
Oracle Communications Cloud Native Environment (CNE)	22.3.0	NA	CNE 22.3.0 supports fresh installation and upgrade from 22.2.x to 22.3.0. For more information on installation, see *Oracle Communications Cloud Native Environment Installation Guide*. For more information on upgrade, see *Oracle Communications Cloud Native Environment Upgrade Guide*.

Table 3-1 (Cont.) Media Pack Contents for Cloud Native Core 2.22.3

Description	NF Version	ATS Version	Upgrade Supported
Oracle Communications Cloud Native Core CD Control Server	22.3.1	NA	CD Control Server 22.3.1 supports fresh installation and upgrade from 22.2.x, 22.3.0 to 22.3.1. For more information on installation, see *Oracle Communications Cloud Native Core CD Control Server Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core CD Control Server	22.3.0	NA	CD Control Server 22.3.0 supports fresh installation and upgrade from 22.2.x to 22.3.0. For more information on installation, see *Oracle Communications Cloud Native Core CD Control Server Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core DBTier	22.3.4	NA	DBTier 22.3.4 supports fresh installation and upgrade from 22.1.x, 22.2.x, and 22.3.x to 22.3.4. For more information on installation, see *Oracle Communications Cloud Native Core DBTier Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core DBTier	22.3.3	NA	DBTier 22.3.3 supports fresh installation and upgrade from 22.1.x, 22.2.x, 22.3.x to 22.3.3. For more information on installation, see *Oracle Communications Cloud Native Core DBTier Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core DBTier	22.3.2	NA	DBTier 22.3.2 supports fresh installation and upgrade from 22.1.x, 22.2.x, 22.3.x to 22.3.2. For more information on installation, see *Oracle Communications Cloud Native Core DBTier Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core DBTier	22.3.1	NA	DBTier 22.3.1 supports fresh installation and upgrade from 22.1.x, 22.2.x, 22.3.0 to 22.3.1. For more information on installation, see *Oracle Communications Cloud Native Core DBTier Installation and Upgrade Guide*.

Table 3-1 (Cont.) Media Pack Contents for Cloud Native Core 2.22.3

Description	NF Version	ATS Version	Upgrade Supported
Oracle Communications Cloud Native Core DBTier	22.3.0	NA	DBTier 22.3.0 supports fresh installation and upgrade from 22.1.x, 22.2.x to 22.3.0. For more information on installation, see *Oracle Communications Cloud Native Core DBTier Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core Policy (CNC Policy)	22.3.4	22.3.4	CNC Policy 22.3.4 supports fresh installation and upgrade from 22.1.x, 22.2.x, and 22.3.x to 22.3.4. For more information on installation or upgrade, see *Oracle Communications Cloud Native Core Converged Policy Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core Policy (CNC Policy)	22.3.3	22.3.1	CNC Policy 22.3.3 supports fresh installation and upgrade from 22.1.x, 22.2.x, and 22.3.x to 22.3.3. For more information on installation or upgrade, see *Oracle Communications Cloud Native Core Converged Policy Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core Policy (CNC Policy)	22.3.2	22.3.1	CNC Policy 22.3.2 supports fresh installation and upgrade from 22.1.x, 22.2.x, and 22.3.x to 22.3.2. For more information on installation or upgrade, see *Oracle Communications Cloud Native Core Converged Policy Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core Policy (CNC Policy)	22.3.1	22.3.1	CNC Policy 22.3.1 supports fresh installation and upgrade from 22.1.x, 22.2.x, and 22.3.0 to 22.3.1. For more information on installation or upgrade, see *Oracle Communications Cloud Native Core Converged Policy Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core Policy (CNC Policy)	22.3.0	22.3.0	CNC Policy 22.3.0 supports fresh installation and upgrade from 22.1.x and 22.2.x to 22.3.0. For more information on installation or upgrade, see *Oracle Communications Cloud Native Core Converged Policy Installation and Upgrade Guide*.

Table 3-1 (Cont.) Media Pack Contents for Cloud Native Core 2.22.3

Description	NF Version	ATS Version	Upgrade Supported
Oracle Communications Cloud Native Core Network Exposure Function (NEF)	22.3.2	22.3.2	NEF 22.3.2 supports fresh installation only. For more information on installation, see *Oracle Communications Cloud Native Core Network Exposure Function Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core Network Exposure Function (NEF)	22.3.1	22.3.1	NEF 22.3.1 supports fresh installation only. For more information on installation, see *Oracle Communications Cloud Native Core Network Exposure Function Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core Network Exposure Function (NEF)	22.3.0	22.3.0	NEF 22.3.0 supports fresh installation only. For more information on installation, see *Oracle Communications Cloud Native Core Network Exposure Function Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core Network Repository Function (NRF)	22.3.2	22.3.3	NRF 22.3.2 supports fresh installation and upgrade from 22.2.x and 22.3.x to 22.3.2. For more information on installation, see *Oracle Communications Cloud Native Core Network Repository Function Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core Network Repository Function (NRF)	22.3.1	22.3.1	NRF 22.3.1 supports fresh installation and upgrade from 22.2.x, 22.3.0 to 22.3.1. For more information on installation, see *Oracle Communications Cloud Native Core Network Repository Function Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core Network Repository Function (NRF)	22.3.0	22.3.0	NRF 22.3.0 supports fresh installation and upgrade from 22.2.x to 22.3.0. For more information on installation, see *Oracle Communications Cloud Native Core Network Repository Function Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core Network Slice Selection Function (NSSF)	22.3.2	22.3.2	NSSF 22.3.2 supports fresh installation and upgrade from 22.2.x and 22.3.x to 22.3.2. For more information on installation, see *Oracle Communications Cloud Native Core Network Slice Selection Function Installation and Upgrade Guide*.

Table 3-1 (Cont.) Media Pack Contents for Cloud Native Core 2.22.3

Description	NF Version	ATS Version	Upgrade Supported
Oracle Communications Cloud Native Core Network Slice Selection Function (NSSF)	22.3.1	22.3.1	NSSF 22.3.1supports fresh installation and upgrade from 22.2.x, 22.3.0 to 22.3.1. For more information on installation, see *Oracle Communications Cloud Native Core Network Slice Selection Function Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core Network Slice Selection Function (NSSF)	22.3.0	22.3.0	NSSF 22.3.0 supports fresh installation and upgrade from 22.2.x to 22.3.0. For more information on installation, see *Oracle Communications Cloud Native Core Network Slice Selection Function Installation and Upgrade Guide*.
Oracle Communications Networks Data Analytics Function (NWDAF)	22.0.0	22.0.0	NWDAF 22.0.0.0.0 supports fresh installation only. For more information on installation, see *Oracle Communications Networks Data Analytics Function Installation Guide*.
Oracle Communications Cloud Native Core Service Communications Proxy (SCP)	22.3.4	22.3.4	SCP 22.3.4 supports fresh installation and upgrade from 22.1.x, 22.2.x, and 22.3.x to 22.3.4. For more information on installation, see *Oracle Communications Cloud Native Core Service Communication Proxy Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core Service Communications Proxy (SCP)	22.3.3	22.3.3	SCP 22.3.3 supports fresh installation and upgrade from 22.1.x, 22.2.x, 22.3.x to 22.3.3. For more information on installation, see *Oracle Communications Cloud Native Core Service Communication Proxy Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core Service Communications Proxy (SCP)	22.3.2	22.3.2	SCP 22.3.2 supports fresh installation and upgrade from 22.1.x, 22.2.x, 22.3.x to 22.3.2. For more information on installation, see *Oracle Communications Cloud Native Core Service Communication Proxy Installation and Upgrade Guide*.

Table 3-1 (Cont.) Media Pack Contents for Cloud Native Core 2.22.3

Description	NF Version	ATS Version	Upgrade Supported
Oracle Communications Cloud Native Core Service Communications Proxy (SCP)	22.3.1	22.3.1	SCP 22.3.1 supports fresh installation and upgrade from 22.1.x, 22.2.x, 22.3.0 to 22.3.1. For more information on installation, see *Oracle Communications Cloud Native Core Service Communication Proxy Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core Service Communications Proxy (SCP)	22.3.0	22.3.0	SCP 22.3.0 supports fresh installation and upgrade from 22.1.x, 22.2.x to 22.3.0. For more information on installation, see *Oracle Communications Cloud Native Core Service Communication Proxy Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core Security Edge Protection Proxy (SEPP)	22.3.2	22.3.2	SEPP 22.3.2 supports fresh installation and upgrade from 22.2.x and 22.3.x to 22.3.2. For more information on installation, see *Oracle Communications Cloud Native Core Security Edge Protection Proxy Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core Security Edge Protection Proxy (SEPP)	22.3.1	22.3.1	SEPP 22.3.1 supports fresh installation and upgrade from 22.2.x, 22.3.0 to 22.3.1. For more information on installation, see *Oracle Communications Cloud Native Core Security Edge Protection Proxy Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core Security Edge Protection Proxy (SEPP)	22.3.0	22.3.0	SEPP 22.3.0 supports fresh installation and upgrade from 22.2.x to 22.3.0. For more information on installation, see *Oracle Communications Cloud Native Core Security Edge Protection Proxy Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core Unified Data Repository (UDR)	22.3.4	22.3.0	UDR 22.3.4 supports fresh installation and upgrade from 22.1.x, 22.2.x, and 22.3.x to 22.3.4. For more information on installation or upgrading, see *Oracle Communications Cloud Native Core United Data Repository Installation and Upgrade Guide*.

Table 3-1 (Cont.) Media Pack Contents for Cloud Native Core 2.22.3

Description	NF Version	ATS Version	Upgrade Supported
Oracle Communications Cloud Native Core Unified Data Repository (UDR)	22.3.3	22.3.1	UDR 22.3.3 supports fresh installation and upgrade from 22.1.x, 22.2.x, and 22.3.x to 22.3.3. For more information on installation or upgrading, see *Oracle Communications Cloud Native Core United Data Repository Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core Unified Data Repository (UDR)	22.3.2	22.3.0	UDR 22.3.2 supports fresh installation and upgrade from 22.1.x, 22.2.x, and 22.3.x to 22.3.2. For more information on installation or upgrading, see *Oracle Communications Cloud Native Core United Data Repository Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core Unified Data Repository (UDR)	22.3.1	22.3.0	UDR 22.3.1 supports fresh installation and upgrade from 22.1.x, 22.2.x, and 22.3.0 to 22.3.1. For more information on installation or upgrading, see *Oracle Communications Cloud Native Core United Data Repository Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core Unified Data Repository (UDR)	22.3.0	22.3.0	UDR 22.3.0 supports fresh installation and upgrade from 1.15.x, 22.1.x, and 22.2.x to 22.3.0. For more information on installation or upgrading, see *Oracle Communications Cloud Native Core United Data Repository Installation and Upgrade Guide*.

3.2 Compliance Matrix

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

Table 3-2 Compliance Matrix

CNC NF	NF Version	OCCNE	DBTier	CDCS	OSO	Kubernetes	CNC Console	3GPP
BSF	22.3.4	• 22.3.x • 22.2.x • 22.1.x	• 22.3.x • 22.2.x • 22.1.x	NA	• 22.3.x • 1.10.x • 1.6.x	• 1.23.x • 1.22.x • 1.21.x	22.3.x	• 3GPP TS 29.521 v16.5.0 • 3GPP TS 33.501 v16.4.0

Table 3-2 (Cont.) Compliance Matrix

CNC NF	NF Version	OCCNE	DBTier	CDCS	OSO	Kubernetes	CNC Console	3GPP
BSF	22.3.2	• 22.3.x • 22.2.x • 22.1.x	• 22.3.x • 22.2.x • 22.1.x	NA	• 22.3.x • 1.10.x • 1.6.x	• 1.23.x • 1.22.x • 1.21.x	22.3.x	• 3GPP TS 29.521 v16.5.0 • 3GPP TS 33.501 v16.4.0
BSF	22.3.0	• 22.3.x • 22.2.x • 22.1.x	• 22.3.x • 22.2.x • 22.1.x	NA	• 22.3.x • 1.10.x • 1.6.x	• 1.23.x • 1.22.x • 1.21.x	22.3.x	• 3GPP TS 29.521 v16.5.0 • 3GPP TS 33.501 v16.4.0
CNC Console	22.3.2	• 22.3.x • 22.2.x • 22.1.x	• 22.3.x • 22.2.x • 22.1.x	22.3.x	• 22.3.x • 1.10.x • 1.6.x	• 1.23.x • 1.22.x • 1.21.x	NA	NA
CNC Console	22.3.1	• 22.3.x • 22.2.x • 22.1.x	• 22.3.x • 22.2.x • 22.1.x	22.3.x	• 22.3.x • 1.10.x • 1.6.x	• 1.23.x • 1.22.x • 1.21.x	NA	NA
CNC Console	22.3.0	• 22.3.x • 22.2.x • 22.1.x	• 22.3.x • 22.2.x • 22.1.x	22.3.x	• 22.3.x • 1.10.x • 1.6.x	• 1.23.x • 1.22.x • 1.21.x	NA	NA
OCCNE	22.3.3	NA	22.3.x	NA	22.3.x	1.23.x	NA	NA
OCCNE	22.3.1	NA	22.3.0	NA	22.3.x	1.23.x	NA	NA
OCCNE	22.3.0	NA	22.3.0	NA	22.3.x	1.23.x	NA	NA

Table 3-2 (Cont.) Compliance Matrix

CNC NF	NF Version	OCCNE	DBTier	CDCS	OSO	Kubernetes	CNC Console	3GPP
CNC Policy	22.3.4	• 22.3.x • 22.2.x • 22.1.x	• 22.3.x • 22.2.x • 22.1.x	NA	• 22.3.x • 1.10.x • 1.6.x	• 1.23.x • 1.22.x • 1.21.x	22.3.x	• 3GPP TS 23.203v15.4.0 • 3GPP TS 23.503v15.7.0 • 3GPP TS 29.500v16.3.0 • 3GPP TS 29.507v15.5.0 • 3GPP TS 29.512v16.4 • 3GPP TS 29.513v15.5.0 • 3GPP TS 29.514v16.4.0 • 3GPP TS 29.514v15.5.0 • 3GPP TS 29.519v15.5.0 • 3GPP TS 29.521v16.5.0 • 3GPP TS 29.525v15.3.0 • 3GPP TS 29.594v15.5.0 • 3GPP TS 29.212v15.4 • 3GPP TS 29.213v15.4 • 3GPP TS 29.214v15.4.0 • 3GPP TS 29.215v15.1.0 • 3GPP TS 29.219v15.1.0 • 3GPP TS 29.329v14.0.0 • 3GPP TS 29.335v13.1.0

Table 3-2 (Cont.) Compliance Matrix

CNC NF	NF Version	OCCNE	DBTier	CDCS	OSO	Kubernetes	CNC Console	3GPP
CNC Policy	22.3.3	• 22.3.x • 22.2.x • 22.1.x	• 22.3.x • 22.2.x • 22.1.x	NA	• 22.3.x • 1.10.x • 1.6.x	• 1.23.x • 1.22.x • 1.21.x	22.3.x	• 3GPP TS 23.203v15.4.0 • 3GPP TS 23.503v15.7.0 • 3GPP TS 29.500v16.3.0 • 3GPP TS 29.507v15.5.0 • 3GPP TS 29.512v16.4 • 3GPP TS 29.513v15.5.0 • 3GPP TS 29.514v16.4.0 • 3GPP TS 29.514v15.5.0 • 3GPP TS 29.519v15.5.0 • 3GPP TS 29.521v16.5.0 • 3GPP TS 29.525v15.3.0 • 3GPP TS 29.594v15.5.0 • 3GPP TS 29.212v15.4 • 3GPP TS 29.213v15.4 • 3GPP TS 29.214v15.4.0 • 3GPP TS 29.215v15.1.0 • 3GPP TS 29.219v15.1.0 • 3GPP TS 29.329v14.0.0 • 3GPP TS 29.335v13.1.0

Table 3-2 (Cont.) Compliance Matrix

CNC NF	NF Version	OCCNE	DBTier	CDCS	OSO	Kubernetes	CNC Console	3GPP
CNC Policy	22.3.2	• 22.3.x • 22.2.x • 22.1.x	• 22.3.x • 22.2.x • 22.1.x	NA	• 22.3.x • 1.10.x • 1.6.x	• 1.23.x • 1.22.x • 1.21.x	22.3.x	• 3GPP TS 23.203v15.4.0 • 3GPP TS 23.503v15.7.0 • 3GPP TS 29.500v16.3.0 • 3GPP TS 29.507v15.5.0 • 3GPP TS 29.512v16.4 • 3GPP TS 29.513v15.5.0 • 3GPP TS 29.514v16.4.0 • 3GPP TS 29.514v15.5.0 • 3GPP TS 29.519v15.5.0 • 3GPP TS 29.521v16.5.0 • 3GPP TS 29.525v15.3.0 • 3GPP TS 29.594v15.5.0 • 3GPP TS 29.212v15.4 • 3GPP TS 29.213v15.4 • 3GPP TS 29.214v15.4.0 • 3GPP TS 29.215v15.1.0 • 3GPP TS 29.219v15.1.0 • 3GPP TS 29.329v14.0.0 • 3GPP TS 29.335v13.1.0

Table 3-2 (Cont.) Compliance Matrix

CNC NF	NF Version	OCCNE	DBTier	CDCS	OSO	Kubernetes	CNC Console	3GPP
CNC Policy	22.3.1	• 22.3.x • 22.2.x • 22.1.x	• 22.3.x • 22.2.x • 22.1.x	NA	• 22.3.x • 1.10.x • 1.6.x	• 1.23.x • 1.22.x • 1.21.x	22.3.x	• 3GPP TS 23.203v15.4.0 • 3GPP TS 23.503v15.7.0 • 3GPP TS 29.500v16.3.0 • 3GPP TS 29.507v15.5.0 • 3GPP TS 29.512v16.4 • 3GPP TS 29.513v15.5.0 • 3GPP TS 29.514v16.4.0 • 3GPP TS 29.514v15.5.0 • 3GPP TS 29.519v15.5.0 • 3GPP TS 29.521v16.5.0 • 3GPP TS 29.525v15.3.0 • 3GPP TS 29.594v15.5.0 • 3GPP TS 29.212v15.4 • 3GPP TS 29.213v15.4 • 3GPP TS 29.214v15.4.0 • 3GPP TS 29.215v15.1.0 • 3GPP TS 29.219v15.1.0 • 3GPP TS 29.329v14.0.0 • 3GPP TS 29.335v13.1.0

Table 3-2 (Cont.) Compliance Matrix

CNC NF	NF Version	OCCNE	DBTier	CDCS	OSO	Kubernetes	CNC Console	3GPP
CNC Policy	22.3.0	22.3.x 22.2.x 22.1.x	22.3.x 22.2.x 22.1.x	NA	22.3.x 1.10.x 1.6.x	1.23.x 1.22.x 1.21.x	22.3.x	• 3GPP TS 23.203v15.4.0 • 3GPP TS 23.503v15.7.0 • 3GPP TS 29.500v16.3.0 • 3GPP TS 29.507v15.5.0 • 3GPP TS 29.512v16.4 • 3GPP TS 29.513v15.5.0 • 3GPP TS 29.514v16.4.0 • 3GPP TS 29.514v15.5.0 • 3GPP TS 29.519v15.5.0 • 3GPP TS 29.521v16.5.0 • 3GPP TS 29.525v15.3.0 • 3GPP TS 29.594v15.5.0 • 3GPP TS 29.212v15.4 • 3GPP TS 29.213v15.4 • 3GPP TS 29.214v15.4.0 • 3GPP TS 29.215v15.1.0 • 3GPP TS 29.219v15.1.0 • 3GPP TS 29.329v14.0.0 • 3GPP TS 29.335v13.1.0
DBTier	22.3.4	22.3.x	NA	NA	22.3.x	1.23.x	NA	NA
DBTier	22.3.3	22.3.1	NA	NA	22.3.x	1.23.x	NA	NA
DBTier	22.3.2	22.3.1	NA	NA	22.3.x	1.23.x	NA	NA
DBTier	22.3.1	22.3.1	NA	NA	22.3.x	1.23.x	NA	NA
DBTier	22.3.0	22.3.0	NA	NA	22.3.x	1.23.x	NA	NA

Table 3-2 (Cont.) Compliance Matrix

CNC NF	NF Version	OCCNE	DBTier	CDCS	OSO	Kubernetes	CNC Console	3GPP
NEF	22.3.2	• 22.3.x • 22.2.x • 22.1.x	• 22.3.x • 22.2.x • 22.1.x	NA	NA	• 1.23.x • 1.22.x • 1.21.x	NA	• 3GPP TS 23.222 v16.9.0 • 3GPP TS 23.501 v16.7.0 • 3GPP TS 23.502 v16.7.0 • 3GPP TS 29.122 v16.8.0 • 3GPP TS 29.222 v16.5.0 • 3GPP 29.500 v16.6.0 • 3GPP 29.501 v16.6.0 • 3GPP TS 29.522 v16.6.0 • 3GPP 29.510 v16.6.0 • 3GPP TS 29.591 v16.3.0 • TS 29.515 v16.7 • TS 29.503 v16.6 • TS 29.521 v16.10 • TS 29.514 v16.10.0

Table 3-2 (Cont.) Compliance Matrix

CNC NF	NF Version	OCCNE	DBTier	CDCS	OSO	Kubernetes	CNC Console	3GPP
NEF	22.3.1	• 22.3.x • 22.2.x • 22.1.x	• 22.3.x • 22.2.x • 22.1.x	NA	NA	• 1.23.x • 1.22.x • 1.21.x	NA	• 3GPP TS 23.222 v16.9.0 • 3GPP TS 23.501 v16.7.0 • 3GPP TS 23.502 v16.7.0 • 3GPP TS 29.122 v16.8.0 • 3GPP TS 29.222 v16.5.0 • 3GPP 29.500 v16.6.0 • 3GPP 29.501 v16.6.0 • 3GPP TS 29.522 v16.6.0 • 3GPP 29.510 v16.6.0 • 3GPP TS 29.591 v16.3.0 • TS 29.515 v16.7 • TS 29.503 v16.6 • TS 29.521 v16.10 • TS 29.514 v16.10.0

Table 3-2 (Cont.) Compliance Matrix

CNC NF	NF Version	OCCNE	DBTier	CDCS	OSO	Kubernetes	CNC Console	3GPP
NEF	22.3.0	• 22.3.x • 22.2.x • 22.1.x	• 22.3.x • 22.2.x • 22.1.x	NA	NA	• 1.23.x • 1.22.x • 1.21.x	NA	• 3GPP TS 23.222 v16.9.0 • 3GPP TS 23.501 v16.7.0 • 3GPP TS 23.502 v16.7.0 • 3GPP TS 29.122 v16.8.0 • 3GPP TS 29.222 v16.5.0 • 3GPP 29.500 v16.6.0 • 3GPP 29.501 v16.6.0 • 3GPP TS 29.522 v16.6.0 • 3GPP 29.510 v16.6.0 • 3GPP TS 29.591 v16.3.0 • TS 29.515 v16.7 • TS 29.503 v16.6 • TS 29.521 v16.10 • TS 29.514 v16.10.0
NRF	22.3.2	• 22.3.x • 22.2.x • 22.1.x	• 22.3.x • 22.2.x • 22.1.x	NA	• 22.3.x • 1.6.x	• 1.23.x • 1.22.x • 1.21.x	22.3.x	• 3GPP TS 29.510, v15.5 • 3GPP TS 29.510 v16.3 • 3GPP TS 29.510 v16.7
NRF	22.3.1	• 22.3.x • 22.2.x • 22.1.x	• 22.3.x • 22.2.x • 22.1.x	NA	• 22.3.x • 1.10.x • 1.6.x	• 1.23.x • 1.22.x • 1.21.x	22.3.x	• 3GPP TS 29.510 v15.5.0 • 3GPP TS 29.510 v16.5.0
NRF	22.3.0	• 22.3.x • 22.2.x • 22.1.x	• 22.3.x • 22.2.x • 22.1.x	NA	• 22.3.x • 1.10.x • 1.6.x	• 1.23.x • 1.22.x • 1.21.x	22.3.x	• 3GPP TS 29.510 v15.5.0 • 3GPP TS 29.510 v16.5.0
NSSF	22.3.2	• 22.3.x • 22.2.x • 22.1.x	• 22.3.x • 22.2.x • 22.1.x	NA	• 22.3.x • 1.10.x • 1.6.x	• 1.23.x • 1.22.x • 1.21.x	22.3.x	• 3GPP TS 29.531 v15.5.0 • 3GPP TS 29.531 v16.5.0

Table 3-2 (Cont.) Compliance Matrix

CNC NF	NF Version	OCCNE	DBTier	CDCS	OSO	Kubernetes	CNC Console	3GPP
NSSF	22.3.1	• 22.3.x • 22.2.x • 22.1.x	• 22.3.x • 22.2.x • 22.1.x	NA	• 22.3.x • 1.10.x • 1.6.x	• 1.23.x • 1.22.x • 1.21.x	22.3.x	• 3GPP TS 29.531 v15.5.0 • 3GPP TS 29.531 v16.5.0
NSSF	22.3.0	• 22.3.x • 22.2.x • 22.1.x	• 22.3.x • 22.2.x • 22.1.x	NA	• 22.3.x • 1.10.x • 1.6.x	• 1.23.x • 1.22.x • 1.21.x	22.3.x	• 3GPP TS 29.531 v15.5.0 • 3GPP TS 29.531 v16.5.0
NWDAF	22.0.0	22.1.0	22.2.0	NA	NA	• 1.23.x • 1.22.x • 1.21.x	NA	• 3GPP TS 23.288 v16 • 3GPP TS 23.288 v17.4.0 • 3GPP TS 29.520 v17.6.0 • 3GPP TS 29.508 v17.5.0 • 3GPP TS 29.518 v17.5.0 • 3GPP TS 23.501 v17.5.0 • 3GPP TS 23.502 v17.4.0 • 3GPP TS 33.521 v17.1.0
SCP	22.3.4	• 22.3.x • 22.2.x • 22.1.x	• 22.3.x • 22.2.x • 22.1.x	22.3.x	• 22.3.x • 1.10.x • 1.6.x	• 1.23.x • 1.22.x • 1.21.x	22.3.x	• 3GPP TS 23.501 v16.7.0 • 3GPP TS 23.502 v16.7.0 • 3GPP TS 29.500 v16.6.0 • 3GPP TS 29.501 v16.5.0 • 3GPP TS 29.510 v16.6.0 • 3GPP TS 33.501 v16.5.0 • 3GPP TS 33.117 v16.6.0 • 3GPP TS 33.210 v16.4.0

Table 3-2 (Cont.) Compliance Matrix

CNC NF	NF Version	OCCNE	DBTier	CDCS	OSO	Kubernetes	CNC Console	3GPP
SCP	22.3.3	• 22.3.x • 22.2.x • 22.1.x	• 22.3.x • 22.2.x • 22.1.x	22.3.x	• 22.3.x • 1.10.x • 1.6.x	• 1.23.x • 1.22.x • 1.21.x	22.3.x	• 3GPP TS 23.501 v16.7.0 • 3GPP TS 23.502 v16.7.0 • 3GPP TS 29.500 v16.6.0 • 3GPP TS 29.501 v16.5.0 • 3GPP TS 29.510 v16.6.0 • 3GPP TS 33.501 v16.5.0 • 3GPP TS 33.117 v16.6.0 • 3GPP TS 33.210 v16.4.0
SCP	22.3.2	• 22.3.x • 22.2.x • 22.1.x	• 22.3.x • 22.2.x • 22.1.x	22.3.x	• 22.3.x • 1.10.x • 1.6.x	• 1.23.x • 1.22.x • 1.21.x	22.3.x	• 3GPP TS 23.501 v16.7.0 • 3GPP TS 23.502 v16.7.0 • 3GPP TS 29.500 v16.6.0 • 3GPP TS 29.501 v16.5.0 • 3GPP TS 29.510 v16.6.0 • 3GPP TS 33.501 v16.5.0 • 3GPP TS 33.117 v16.6.0 • 3GPP TS 33.210 v16.4.0
SCP	22.3.1	• 22.3.x • 22.2.x • 22.1.x	• 22.3.x • 22.2.x • 22.1.x	22.3.x	• 22.3.x • 1.10.x • 1.6.x	• 1.23.x • 1.22.x • 1.21.x	22.3.x	• 3GPP TS 23.501 v16.7.0 • 3GPP TS 23.502 v16.7.0 • 3GPP TS 29.500 v16.6.0 • 3GPP TS 29.501 v16.5.0 • 3GPP TS 29.510 v16.6.0 • 3GPP TS 33.501 v16.5.0 • 3GPP TS 33.117 v16.6.0 • 3GPP TS 33.210 v16.4.0

Table 3-2 (Cont.) Compliance Matrix

CNC NF	NF Version	OCCNE	DBTier	CDCS	OSO	Kubernetes	CNC Console	3GPP
SCP	22.3.0	• 22.3.x • 22.2.x • 22.1.x	• 22.3.x • 22.2.x • 22.1.x	22.3.x	• 22.3.x • 1.10.x • 1.6.x	• 1.23.x • 1.22.x • 1.21.x	22.3.x	• 3GPP TS 23.501 v16.7.0 • 3GPP TS 23.502 v16.7.0 • 3GPP TS 29.500 v16.6.0 • 3GPP TS 29.501 v16.5.0 • 3GPP TS 29.510 v16.6.0 • 3GPP TS 33.501 v16.5.0 • 3GPP TS 33.117 v16.6.0 • 3GPP TS 33.210 v16.4.0
SEPP	22.3.2	• 22.3.x • 22.2.x • 22.1.x	• 22.3.x • 22.2.x • 22.1.x	22.3.x	NA	• 1.23.x • 1.22.x • 1.21.x	22.3.x	• 3GPP TS 23.501 v16.7.0 • 3GPP TS 23.502 v16.7.0 • 3GPP TS 29.500 v16.6.0 • 3GPP TS 29.501 v16.5.0 • 3GPP TS 29.510 v16.6.0 • 3GPP TS 29.573 v16.3.0
SEPP	22.3.1	• 22.3.x • 22.2.x • 22.1.x	• 22.3.x • 22.2.x • 22.1.x	22.3.x	NA	• 1.23.x • 1.22.x • 1.21.x	22.3.x	• 3GPP TS 23.501 v16.7.0 • 3GPP TS 23.502 v16.7.0 • 3GPP TS 29.500 v16.6.0 • 3GPP TS 29.501 v16.5.0 • 3GPP TS 29.510 v16.6.0 • 3GPP TS 29.573 v16.3.0

Table 3-2 (Cont.) Compliance Matrix

CNC NF	NF Version	OCCNE	DBTier	CDCS	OSO	Kubernetes	CNC Console	3GPP
SEPP	22.3.0	• 22.3.x • 22.2.x • 22.1.x	• 22.3.x • 22.2.x • 22.1.x	22.3.x	NA	• 1.23.x • 1.22.x • 1.21.x	22.3.x	• 3GPP TS 23.501 v16.7.0 • 3GPP TS 23.502 v16.7.0 • 3GPP TS 29.500 v16.6.0 • 3GPP TS 29.501 v16.5.0 • 3GPP TS 29.510 v16.6.0 • 3GPP TS 29.573 v16.3.0
UDR	22.3.4	• 22.3.x • 22.2.x • 22.1.x	• 22.3.x • 22.2.x • 22.1.x	NA	• 22.3.x • 1.10.x • 1.6.x	• 1.23.x • 1.22.x • 1.21.x	22.3.x	• 3GPP TS 29.505 v15.4.0 • 3GPP TS 29.504 v16.2.0 • 3GPP TS 29.519 v16.2.0 • 3GPP TS 29.511 v17.2.0.
UDR	22.3.3	• 22.3.x • 22.2.x • 22.1.x	• 22.3.x • 22.2.x • 22.1.x	NA	• 22.3.x • 1.10.x • 1.6.x	• 1.23.x • 1.22.x • 1.21.x	22.3.x	• 3GPP TS 29.505 v15.4.0 • 3GPP TS 29.504 v16.2.0 • 3GPP TS 29.519 v16.2.0 • 3GPP TS 29.511 v17.2.0.
UDR	22.3.2	• 22.3.x • 22.2.x • 22.1.x	• 22.3.x • 22.2.x • 22.1.x	NA	• 22.3.x • 1.10.x • 1.6.x	• 1.23.x • 1.22.x • 1.21.x	22.3.x	• 3GPP TS 29.505 v15.4.0 • 3GPP TS 29.504 v16.2.0 • 3GPP TS 29.519 v16.2.0 • 3GPP TS 29.511 v17.2.0.
UDR	22.3.1	• 22.3.x • 22.2.x • 22.1.x	• 22.3.x • 22.2.x • 22.1.x	NA	• 22.3.x • 1.10.x • 1.6.x	• 1.23.x • 1.22.x • 1.21.x	22.3.x	• 3GPP TS 29.505 v15.4.0 • 3GPP TS 29.504 v16.2.0 • 3GPP TS 29.519 v16.2.0 • 3GPP TS 29.511 v17.2.0.

Table 3-2 (Cont.) Compliance Matrix

CNC NF	NF Version	OCCNE	DBTier	CDCS	OSO	Kubernetes	CNC Console	3GPP
UDR	22.3.0	• 22.3.x • 22.2.x • 22.1.x	• 22.3.x • 22.2.x • 22.1.x	NA	• 22.3.x • 1.10.x • 1.6.x	• 1.23.x • 1.22.x • 1.21.x	22.3.x	• 3GPP TS 29.505 v15.4.0 • 3GPP TS 29.504 v16.2.0 • 3GPP TS 29.519 v16.2.0 • 3GPP TS 29.511 v17.2.0.

3.3 Common Microservices Load Lineup

This section provides information about common microservices and ATS for the specific NF versions in Cloud Native Core Release 2.22.3.

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	22.3.4	22.3.13	22.3.4	1.11	22.3.4	22.3.4	22.3.2	22.3.13	22.3.13	22.3.3	NA	22.3.5	22.3.4
BSF	22.3.2	22.3.9	22.3.2	1.11	22.3.1	22.3.2	22.3.1	22.3.9	22.3.9	22.3.2	NA	22.3.4	22.3.2
BSF	22.3.0	22.3.4	22.3.0	22.3.0	22.3.0	22.3.0	22.3.0	22.3.4	22.3.4	22.3.1	NA	22.3.2	22.3.0
CNC Console	22.3.2	NA	NA	NA	NA	NA	22.3.2	NA	22.3.13	22.3.3	NA	NA	NA
CNC Console	22.3.1	NA	NA	NA	NA	NA	22.3.1	NA	22.3.10	22.3.2	NA	NA	NA
CNC Console	22.3.0	NA	NA	NA	NA	NA	22.3.0	NA	22.3.4	22.3.1	NA	NA	NA
CNC Policy	22.3.4	22.3.13	22.3.4	1.11	22.3.4	22.3.4	22.3.2	22.3.13	22.3.13	22.3.3	NA	22.3.5	22.3.4
CNC Policy	22.3.3	22.3.9	22.3.2	1.11	22.3.1	22.3.2	22.3.1	22.3.9	22.3.9	22.3.2	NA	22.3.4	22.3.2
CNC Policy	22.3.2	22.3.9	22.3.2	1.11	22.3.1	22.3.2	22.3.1	22.3.9	22.3.9	22.3.2	NA	22.3.4	22.3.2
CNC Policy	22.3.1	22.3.7	22.3.1	22.3.1	22.3.0	22.3.1	22.3.0	22.3.7	22.3.7	22.3.1	NA	22.3.2	22.3.1
CNC Policy	22.3.0	22.3.4	22.3.0	22.3.0	22.3.0	22.3.0	22.3.0	22.3.4	22.3.4	22.3.1	NA	22.3.2	22.3.0
NEF	22.3.2	NA	22.3.4	NA	22.3.2	22.3.4	22.3.2	22.3.13	22.3.13	22.3.3	NA	22.3.5	22.3.4
NEF	22.3.1	NA	22.3.2	NA	22.3.1	22.3.2	22.3.1	22.3.8	22.3.8	22.3.2	NA	22.3.3	22.3.2
NEF	22.3.0	NA	22.3.0	NA	22.3.0	22.3.0	22.3.0	22.3.3	22.3.3	22.3.0	NA	22.3.1	22.3.0

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

CNC NF	NF Version	Alternate Route Svc	App-Info	ASM Configuration	ATS Framework	Config-Server	Debug-tool	Egress Gateway	Ingress Gateway	Helm Test	Mediation	NRF-Client	Perf-Info
NRF	22.3.2	22.3.13	22.3.4	22.3.0	22.3.2	NA	22.3.2	22.3.13	22.3.13	22.3.3	NA	NA	22.3.4
NRF	22.3.1	22.3.10	22.3.2	22.3.0	22.3.1	NA	22.3.1	22.3.10	22.3.10	22.3.2	NA	NA	22.3.2
NRF	22.3.0	22.3.6	22.3.0	22.3.0	22.3.0	NA	22.3.0	22.3.6	22.3.6	22.3.1	NA	NA	22.3.0
NSSF	22.3.2	NA	22.3.4	22.3.0	22.3.2	NA	22.3.2	22.3.12	23.2.12	22.3.3	NA	22.3.5	22.3.4
NSSF	22.3.1	NA	22.3.2	22.3.0	22.3.1	NA	22.3.1	22.3.9	22.3.9	22.3.2	NA	22.3.2	22.3.0
NSSF	22.3.0	NA	22.3.0	22.3.0	22.3.0	NA	22.3.0	22.3.4	22.3.4	22.3.0	NA	22.3.2	22.3.0
NWDAF	22.0.0	NA	NA	NA	22.1.0	NA	NA	22.3.4	22.3.4	NA	NA	NA	NA
SCP	22.3.4	NA	NA	22.3.0	22.3.2	NA	22.3.2	NA	NA	22.3.3	22.3.3	NA	NA
SCP	22.3.3	NA	NA	22.3.0	22.3.1	NA	22.3.1	NA	NA	22.3.2	22.3.2	NA	NA
SCP	22.3.2	NA	NA	22.3.0	22.3.1	NA	22.3.1	NA	NA	22.3.2	22.3.2	NA	NA
SCP	22.3.1	NA	NA	22.3.0	22.3.1	NA	22.3.1	NA	NA	22.3.2	22.3.2	NA	NA
SCP	22.3.0	NA	NA	NA	22.3.0	NA	22.3.0	NA	NA	22.3.0	22.3.0	NA	NA
SEPP	22.3.2	NA	22.3.4	NA	22.3.2	22.3.4	22.3.2	22.3.13	22.3.13	22.3.3	22.3.3	22.3.5	22.3.3
SEPP	22.3.1	NA	22.3.2	NA	22.3.1	22.3.2	22.3.1	22.3.9	22.3.9	22.3.1	22.3.0	22.3.1	22.3.0
SEPP	22.3.0	NA	22.3.0	NA	22.3.0	22.3.0	22.3.0	22.3.4	22.3.4	22.3.1	22.3.0	22.3.1	22.3.0
UDR	22.3.4	22.3.13	22.3.4	NA	22.3.2	22.3.4	22.3.2	22.3.13	22.3.13	22.3.3	NA	22.3.5	22.3.4
UDR	22.3.3	22.3.9	22.3.2	NA	22.3.1	22.3.2	22.3.1	22.3.9	22.3.9	22.3.2	NA	22.3.3	22.3.2
UDR	22.3.2	22.3.4	22.3.0	NA	22.3.0	22.3.0	22.3.0	22.3.4	22.3.4	22.3.1	NA	22.3.2	22.3.0
UDR	22.3.1	22.3.4	22.3.0	NA	22.3.0	22.3.0	22.3.0	22.3.4	22.3.4	22.3.1	NA	22.3.2	22.3.0
UDR	22.3.0	22.3.4	22.3.0	NA	22.3.0	22.3.0	22.3.0	22.3.4	22.3.4	22.3.1	NA	22.3.2	22.3.0

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	22.3.4	Jan 10, 2023	Jan 10, 2023	Jan 4, 2023	Dec 12, 2022
BSF	22.3.2	Oct 18, 2022	Oct 17, 2022	Oct 18, 2022	Oct 19, 2022
BSF	22.3.0	Aug 15, 2022	Aug 12, 2022	Aug 12, 2022	Aug 8, 2022

Table 3-4 (Cont.) Security Certification Declaration

CNC NF	NF Version	Systems test on functional and security features	Regression testing on security configuration	Vulnerability testing	Fuzz testing on external interfaces
CNC Console	22.3.2	Aug 10, 2022	Jan 6, 2023	Jan 6, 2023	Aug 10, 2022
CNC Console	22.3.1	Aug 10, 2022	Oct 19, 2022	Oct 17, 2022	Aug 10, 2022
CNC Console	22.3.0	Aug 10, 2022	Aug 25, 2022	Aug 10, 2022	Aug 10, 2022
CNC Policy	22.3.4	Jan 10, 2023	Jan 10, 2023	Jan 4, 2023	Dec 12, 2022
CNC Policy	22.3.3	Nov 7, 2022	Nov 10, 2022	Nov 10, 2022	Nov 1, 2022
CNC Policy	22.3.2	Oct 18, 2022	Oct 17, 2022	Oct 18, 2022	Oct 19, 2022
CNC Policy	22.3.1	Sep 15, 2022	Sep 15, 2022	Sep 15, 2022	Aug 29, 2022
CNC Policy	22.3.0	Aug 15, 2022	Aug 12, 2022	Aug 12, 2022	Aug 8, 2022
NEF	22.3.2	Jan 12, 2023	Jan 12, 2023	Jan 12, 2023	Aug 09, 2022
NEF	22.3.1	Oct 07, 2022	Oct 07, 2022	Oct 07, 2022	Aug 09, 2022
NEF	22.3.0	Aug 09, 2022	Aug 09, 2022	Aug 09, 2022	Aug 09, 2022
NRF	22.3.2	Jan 17, 2023	Oct 17, 2022	Oct 17, 2022	Aug 11, 2022
NRF	22.3.1	Oct 10, 2022	Oct 10, 2022	Oct 10, 2022	Aug 11, 2022
NRF	22.3.0	Aug 11, 2022	Aug 11, 2022	Aug 11, 2022	Aug 11, 2022
NSSF	22.3.2	Jan 10, 2023	Jan 10, 2023	Jan 10, 2023	Jan 10, 2023
NSSF	22.3.1	Oct 12, 2022	Oct 12, 2022	Oct 12, 2022	Oct 12, 2022
NSSF	22.3.0	Aug 11, 2022	Aug 11, 2022	Aug 11, 2022	Aug 11, 2022
NWDAF	22.0.0	Aug 29, 2022	Aug 22, 2022	Aug 22, 2022	Aug 22, 2022
SCP	22.3.4	Jan 12, 2023	Jan 12, 2023	Jan 12, 2023	Jan 12, 2023
SCP	22.3.3	Oct 20, 2022	Oct 20, 2022	Oct 20, 2022	Oct 20, 2022
SCP	22.3.2	Oct 20, 2022	Oct 20, 2022	Oct 20, 2022	Oct 20, 2022
SCP	22.3.1	Oct 20, 2022	Oct 20, 2022	Oct 20, 2022	Oct 20, 2022
SCP	22.3.0	Aug 22, 2022	Aug 22, 2022	Aug 22, 2022	Aug 22, 2022
SEPP	22.3.2	Jan 16, 2023	Jan 16, 2023	Jan 9, 2023	Jan 16, 2023
SEPP	22.3.1	Oct 14, 2022	Oct 14, 2022	NA	NA
SEPP	22.3.0	Aug 22, 2022	Aug 22, 2022	Aug 22, 2022	Aug 22, 2022
UDR	22.3.4	NA (No new security features)	Jan 13, 2023	Jan 13, 2023	Jan 13, 2023
UDR	22.3.3	NA (No new security features)	Oct 07, 2022	Oct 07, 2022	Oct 07, 2022
UDR	22.3.2	NA (No new security features)	Aug 16, 2022	Aug 16, 2022	Aug 16, 2022

Table 3-4 (Cont.) Security Certification Declaration

CNC NF	NF Version	Systems test on functional and security features	Regression testing on security configuration	Vulnerability testing	Fuzz testing on external interfaces
UDR	22.3.1	NA (No new security features)	Aug 16, 2022	Aug 16, 2022	Aug 16, 2022
UDR	22.3.0	NA (no new security features)	Aug 16, 2022	Aug 16, 2022	Aug 16, 2022

3.5 Documentation Pack

All documents for Cloud Native Core (CNC) 2.22.3 are available for download on SecureSites and MOS.

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

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

4
Resolved and Known Bugs

This chapter lists the resolved and known bugs for Cloud Native Core release 2.22.3.

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

4.1 Severity Definitions

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

Severity 1

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

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

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

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

Severity 2

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

Severity 3

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

Severity 4

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

4.2 Resolved Bug List

The following Resolved Bugs tables list the bugs that are resolved in Cloud Native Release 2.22.3.

4.2.1 BSF Resolved Bugs

BSF 22.3.4 Resolved Bugs

There are no resolved bugs in this release.

Table 4-1 BSF 22.3.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
34640002	In custom values yaml, EGW oauthClient::nfInstanceId has non-default value causing user-agent ATS to fail	The default NF instance ID needs an update in custom values yaml file.	3	22.3.0
34724043	BSF System Name is Hard-coded under CM Service which prevents enabling of Controlled Shutdown Feature	BSF system name is not exposed in custom values yaml and Controlled Shutdown feature mandates to the System name to have string of "bsf".	3	22.3.0

Table 4-2 BSF 22.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
34497714	Diam-GW running out of memory in 22.2.0 due to peer config issues.	The Diam GW related ATS test case is failing.	3	22.2.0
34374174	Alerts config files moved from Artifacts to Artifacts/Scripts for Orchestration	AlertConfig file is placed under the Artifacts directory instead of the Artifacts/Scripts.	3	22.2.0

Table 4-2 (Cont.) BSF 22.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
34542204	Helm chart discrepancy for BSF	On deploying BSF 22.1.2. it was observed that the AppVersion field is missing in the helm chart (chart.yaml), which differs from the other NFs.	3	22.1.2
34275940	BSF session viewer query of /128 IPv6 addr is expected to match with the /64 IPv6 addr session like Rx query does	BSF session viewer query of /128 IPv6 addr is expected to match with the /64 IPv6 addr session, like the Rx query.	3	1.11.0

Note:

The resolved bugs from BSF Release 22.2.1 and 22.2.3 are forward ported to Release 22.3.0.

4.2.2 CNC Console Resolved Bugs

Table 4-3 CNC Console 22.3.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34908899	Restart of CNCC mcore-ingress-gateway is expected during rollback procedure from 22.4.0 to 22.3.0 must be documented.	The mcore-ingress-gateway pod gets restarted multiple times during rollback, upgrade, and fresh installation. This behavior was documented in the CNC Console Installation and Upgrade guide for fresh installation and upgrade, but not for rollback. The CNC Console Installation and Upgrade guide has been updated to reflect the restart behavior during the rollback procedure as well.	3	22.4.0
34944868	CNCC CSAR file Definitions/ occncc.yaml file has invalid yaml	The yaml validation is failing in the occncc.yaml file and the CSAR packaging is not getting fully scanned. The following change has been implemented as a part of the fix: Included double quotes for the content in the occncc.yaml file and validated it using the yaml validator.	3	22.3.0

Table 4-4 CNC Console 22.3.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34712597	CNCC 22.2.1 "cncc_vfnd.mf" file Corrections Requested	Customer specific CSAR file has a couple of errors that the customer has to correct before they can install the CNCC. The following changes are updated as part of the fix. line 5: "vnf_release_data_time" is updated as "vnf_release_date_time" line 6: white space is removed. re-add line 6 as delimiter for the first section, with only the newline/linefeed.	3	22.2.1
34598350	CNCC Upgrade procedure to include cncc core uninstall commands	Include CNCC core uninstall commands in CNCC Upgrade procedure. CNC Console Installation and Upgrade guide needs to be updated.	3	22.3.0
34693582	CS_WRITE Role Mapping issues with PCF	CS_WRITE must be enabled to stop access to all Policy entries.	3	22.1.0
34597695	Doc updates to indicate occncc-mcore-ingress-gateway getting restarted during installation	occncc-mcore-ingress-gateway pod is getting restarted, during the installation as the connection with iam-ingress-gateway is not getting established.	3	22.3.0

Table 4-5 CNC Console 22.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34486968	CNCC 22.2.1 "cncc_vfnd.mf" file Corrections Requested	Customer specific CSAR file has a couple of errors that the customer has to correct before they can install the CNCC. The following changes are updated as part of the fix. line 5: "vnf_release_data_time" is updated as "vnf_release_date_time" line 6: white space is removed.	3	22.2.1
34487007	CNC Console is having hanging issues at static.oracle.com	Logging into CNC Console Core takes a very long time. It is because CNCC attempts to reach static.oracle.com. It takes 30 - 60 seconds or more. Or it requires multiple stops and refreshes.	3	22.1.2
34527367	User guide update to include REST API curl commands	Update the CNC Console User Guide REST API section to include curl commands to configure CNCC-IAM for setting CNCC redirection URL and creating users and assigning roles.	3	22.2.0
34455613	Metrics Instance Identifier must be unique	Console helm chart expects unique metrics Instance Identifier for each component. The CNC Console User Guide is updated to reflect the metrics instance identifier must be unique.	4	22.2.0

Table 4-5 (Cont.) CNC Console 22.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34473275	CNCC custom values file to hide static port configuration	CNC Console custom values have a static port configuration which is not used for production deployment but has to be hidden from custom values. The changes are implemented and in case a static port config is needed, it can be updated manually as it is still supported by the console chart.	4	22.2.0
34481785	CNCC 22.2.1 MIB TC textual convention files missing END statement	CNCC 22.2.1 cncc_mib_tc_22.2.1.mib MIB file is missing the END statement. The file has been updated with END statement to resolve the issue.	4	22.2.1

Note:

Resolved bugs from 22.2.1 have been forward ported to Release 22.3.0.

4.2.3 DBTier Resolved Bugs

Table 4-6 cnDBTier 22.3.4 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34644803	CNE and cnDBTier 22.2.1 MIB TC textual convention files missing END statement	OCDBTIER-MIB-TC.MIB.txt file had BEGIN statement but missed the required END statement.	3	22.2.1
34623170	cnDB 22.3.0 ndbmysqld pod restart and replication channel stuck with error "the incident LOST_EVENTS occurred on the master. Message: mysqld startup"	cnDBTier 22.3.0 ndbmysqld pods restarted and the replication channel was stuck during cnPCRF upgrade with the "the incident LOST_EVENTS occurred on the master. Message: mysqld startup" error.	3	22.3.0

Table 4-7 cnDBTier 22.3.3 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34757053	cnDBTier 22.3.0 - Helm test failed for cnDBTier after successful install.	Helm test was not working when ndbmysqld replica count is 0.	3	22.3.0
34822830	Configure required annotations for LoadBalancer services in vCNE for ndbmysqld and DB replication service pods	Bug to configure required annotations for LoadBalancer services in vCNE for ndbmysqld and DB replication service pods.	3	22.2.0
34822848	Configuration for enabling/ disabling the extra logging for replication sql pods.	Configuration for enabling and disabling the extra logging for replication SQL pods.	3	22.2.0
34867168	Uplift MySQL Cluster to [version 8.0.30]	Bug to uplift MySQL Cluster to [version 8.0.30].	3	22.2.0
34770538	In ASM enabled 4 Site GR Setup for CNDB site addition, DR stuck in BACKUPRESTORE state.	New columns' position mismatched between the upgrade and fresh install.	2	22.3.2
34796778	On an upgraded cndb setup from 22.2.2 to 22.3.2 when upgrade is done from 22.3.2 single channel to multi channel, mysql.ndb_replication table is not existing	mysql.ndb_replication table was not present when DBTier was upgraded from version 22.2.x to 22.3.2.	2	22.3.0
34724235	NODE DOWN ALERT in PCF Production Network	Configure management pods (ndbmgmd) to always read the configuration from the configuration file instead of configuration cache.	2	22.1.2

Table 4-8 cnDBTier 22.3.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34735838	DB Tier upgrade failure when upgrading from 22.1.3 to 22.3.0	After attempt to Upgrade to 22.3.0, georedudancy sites were out of sync with errors.	2	22.1.3

Table 4-9 cnDBTier 22.3.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34670943	Use latest Ol8+JDK base image OL86s220923| JDK17.0.4.1 in all cnDBTier k8 services	The base image of Ol8+JDK in all cnDBTier k8 services must be updated to the latest OL86s220923| JDK17.0.4.1 version.	3	22.2.2

Table 4-9 (Cont.) cnDBTier 22.3.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34670991	Input cronjob expression for routine backups	The db-backup-manager-svc can only schedule routine backupsbased on the number of days defined in values.yaml. Consequently, the usercannot specify any specific time for the routine backup to be performed.	3	22.2.1
34648099	Changing the timezone on Pods	The time zones on pods are different in different areas. The predefined timezones must be removed from db-backup-manager-svc.	3	22.1.1
34323097	Change the DB Tier App Version to 5 digit number	DBTier App version shows three digits instead of five digits.	3	22.1.0
34625121	DR stuck at 'CHECK_BACKUP_COPY' state in 4-site setup on Baremetal Cluster	While transferring large backups, db-backup-manager-svc gets a timeout error.	3	22.2.0
34648380	cnDBTier 22.1.1 - Updates Requested In CSAR MF File	The cnDBTier CSAR MF file has typos that that are, at present, manually corrected.	3	22.2.1
34648410	Dish: PCF DR does not restore all data unless mysql.ndb_replication is truncated first.	PCF DR does not restore all data unless mysql.ndb_replication is truncated first.	3	22.1.1
34648102	PI-B 2022 cnDBTier Package cannot be scanned due to undefined alias 'descriptor_id'	cnDBTier Package is not able to be scanned due to undefined alias 'descriptor_id'.	3	22.2.0
34632335	Manual restart of NDB cluster is required after helm upgrade to ensure new sql pods join the cluster in Conversion procedure	All the pods are not restarted after helm upgrade in the 'Conversion of Single Replication Channel Group to Multi Replication Channel Groups' procedure. Manual restart of NDB cluster is required after helm upgrade to ensure new SQL pods join the cluster in the conversion procedure.	3	22.3.0

Table 4-10 cnDBTier 22.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34308341	Allowing the Disaster recovery of cnDBTier clusters even if the cluster2 and cluster3 are getting reinstalled without cluster1	Automated DR is stuck in the initial state and automated DR is triggered again if cnDBTier cluster2 and cluster3 are made as mated pairs in a three site setup without installing the cnDBTier cluster1.	2	22.1.1
34484443	Dual stack support for db-backup-manager-svc	The db-backup-manager-svc HTTP server does not support ipv6, and therefore Db-backup-manager-svc is not running in the ipv6 cluster.	3	22.2.0
34484422	Fix the monitor svc so that it will not use the "ndbmysqldsvc" when apiReplicaCount=0	An unnecessary error message is printed in the monitor svc when the connection to the database is not there. The non-real-time local status API gives the wrong output because of this issue.	3	22.1.0
34491315	Fix the manifest file in the vzw CSAR package for cnDBTier	The variable name "vnf_release_data_time" is incorrect in the manifest file in the cnDBTier vzw CSAR package. Due to this, the CSAR validation fails at the customer site.	3	22.2.1
34484432	Remove the non used configurations from the values.yaml file for replication svc	cnDBTier default and custom_values.yaml file has some configurations for replication svc that are not used in the helm chart. These settings confuses the user and therefore need to be removed from the values.yaml file.	4	22.1.1

> **Note:**
>
> Resolved bugs from 22.2.1 and 22.2.2 have been forward ported to Release 22.3.0.

4.2.4 CDCS Resolved Bugs

CDCS Release 22.3.1

There are no resolved bugs in CDCS Release 22.3.1.

Table 4-11 CDCS 22.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34501825	Unable to adopt existing VmWare sites	An error, "*Unsupported infrastructure 'vcd'*", is thrown while adopting a VmWare site.	3	22.1.0, 22.2.0
34501842	Absence of yaml module in vmware	On CNE upgrade in VmWare set up, "Manage Existing Production Site" pipeline fails because of absence of yaml module in VmWare.	3	22.1.0, 22.2.0

4.2.5 CNE Resolved Bugs

Table 4-12 CNE 22.3.3 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34644768	OCCNE K8S_UPGRADE FAILING 22.1.0 failing	The OCCNE K8S_UPGRADE FAILING 22.1.0 process failed even after deleting the PDB "disruptionbudgets" pod.	3	22.1.0 22.2.0 22.3.0 22.4.0

Table 4-13 CNE 22.3.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34644811	/var/log/messages file size zero	In the provision log_config task, we set a postrotate script for the logrotate program. This postrotate script is supposed to get rsyslog to reload the `/var/log/messages` and other file handles after rotation, but it is not functioning as expected. This bug impacts all hosts or VMs of baremetal and virtual OCCNE instances.	3	22.1.2,22.2.1,22.3.0
34650732	Improve OCCNE deployment time for large clusters	As systems scale up in number of nodes, the deployment time increases significantly.	3	22.1.2,22.2.1,22.3.0

Table 4-13 (Cont.) CNE 22.3.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34650767	The addWorker.py script failed on openstack.	The addWorkerNode.py script fails to add a worker node in openstack. A new worker node cannot be added as per the maintenance procedure.	3	22.3.0,22.4.0

Table 4-14 CNE 22.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34480047	OCCNE - BM Not all services reachable by External IP	Not all services listed as having external IP addresses are reachable in baremetal deployments of 22.2.0. This causes installation failure at services verification.	3	22.2.0
34480168	OCCNE OpenStack LBVMs not able to get NTP sync from bastion	Load Balancer VM instances do not sync their time with the chrony NTP server on the bastion. This appears due to the restrictive security-rules in the LBVM security groups.	3	1.10.2 1.10.3 22.1.0 22.2.0
34480237	When add new nodes, the /etc/hosts files in the servers have unexpected entries or missing new entries.	Users are unable to access Kubernetes worker nodes by name from the Bastion Host.	3	1.8.4 1.9.0 22.1.0 22.2.0
33853995	jaeger logs are rejected by Elasticsearch because of "ts" field mismatch	Jaeger logs are rejected by Elasticsearch because of "ts" field mismatch.	3	1.8.4 1.9.0 1.10.0

Table 4-15 OSO 22.3.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34734944	OSO CSAR file failed to upload in NFVD.	cpuResourceRequest must be float value in VNFD.	2	22.3.1

OSO Release 22.3.1

There are no resolved bugs.

OSO Release 22.3.0

There are no resolved bugs.

4.2.6 CNC Policy Resolved Bugs

CNC Policy 22.3.4 Resolved Bugs

There are no resolved bugs in this release.

Table 4-16 CNC Policy 22.3.3 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
34797295	AM-service not passing user data to PRE pod	For AM-calls, AM service is unable to pass the user data to PRE after the AM data is fetched by PDS for the given subscriber.	1	22.3.2
34798542	Rx policy issue with Override attributes	When processing Rx mediaTypes, PRE sends the correct QOS information related to ARP to SM. However, SM is overriding those values with default values.	1	22.3.2
34789065	PCF 503 Errors due to BSF Target API root header showing NULL	Binding pod is unable to discover BSF if bsfinfo is not contained in the BSF registered profile. This results in BSF binding registration BSF set with "3gpp-sbi-target-apiroot=[null://null]"	2	22.3.2

Table 4-17 CNC Policy 22.3.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
34644505	PCF 5G voice calls not working after upgrade to PIC	On every AAR-I/U for the same subscriber, during QoS Data calculations, the original referenced qosData object was getting modified. This kept on reducing the bandwidth values for the Rx flows for subsequent Rx requests using this referenced qosData object.	2	22.3.0
34593628	UE-PCF responding to POST create request with 200 OK	PCF is responding to AMF with 200 when UE-Create processing does not find an AMF profile.	2	22.2.3
34709104	Issues seen during cncp upgrade from 22.1.2 to 22.3.1	PDS and Binding service schema changed and an upgrade needs to handle the changes.	2	22.3.1
34668189	multiple internet sm sessions in database, expected only 1 session per dnn	Based on Policy design, PCF needs the ability to update BSF with pcfBindings registration based on DNNs.	3	22.2.3
34674124	PCF application not adding maker to RAR messages	In the PCF logs, the RAR is seen, and the call flow pcap also looks good, but in the diam-conn we do not see a marker tag associated with the RAR.	3	22.2.3

Table 4-17 (Cont.) CNC Policy 22.3.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
34724043	PCF System Name is Hard-coded under CM Service which prevents enabling of Controlled Shutdown Feature	PCF system name is not exposed in custom values yaml and Controlled Shutdown feature mandates the System name to have a string of either "pcf" or "cnc policy".	3	22.3.0

Table 4-18 CNC Policy 22.3.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
34648280	nUDR messaging failure - EGW tcp window size 0	Threading model in EGW caused traffic to be blocked at certain ports causing TCP Window to become 0 and all traffic to timeout.	2	22.2.2
34645664	PCF not honoring preferred locality when performing its UDR selection	In PCF, “priority” at NFService level is not considered for UDR profile selection. Instead, “priority” at NFProfile level is considered. In case of all NfProfiles having same priority causes selecting one of the UDR NFProfiles randomly.	2	22.1.1
34645681	PRE debug logs do not show Policy evaluation for UE svc call	The policy execution steps for UE Policy svc call are not observed when PRE is in DEBUG mode.	2	22.2.3

Table 4-18 (Cont.) CNC Policy 22.3.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
34645624	Diamgw pod context onwer query to Binding Pod fails with cancellationException	The POST binding request for context owner query from diam-gw timed out because TCP connections between diamgw pod & binding pods either are stuck or down.	2	1.15.5
34644896	PCRF-Core not responding to some ASRs due to deleting the session twice	There is a race condition in pcrf-core between CCR-U/T initiated ASR and corresponding STR if all messages are received on the same pod. In this case, STR is not responded by pcrf-core, causes diam-gw to respond with DIAMETER_UNABLE_TO_DELIVER for that STR.	3	22.3.0
34645592	Logging Level ERRROR on PCF GUI for PCRF core does not result in correct logging level in Pod logs	The logging level change for pcrf-core in CM GUI is getting reflected in an internal jar/ library (pcrf-common) causing the library logs to stay at the default i.e. WARN level.	3	22.3.0, 22.2.0, 22.1.0, and 1.15.1
34559422	PTI value is 0 in UE N1_N2 Message delivery	UE service sends "0" constant PTI value in NAS Encoded Message to AMF. Instead a variable/ incremental PTI value (starting from 80H to FEH) should be sent for every UE policy association create/ updated.	3	22.3.0

Table 4-18 (Cont.) CNC Policy 22.3.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
34559546	CNCP replying with success in SNA, Even after Sy session already terminated with STR/STA	If OCS routes a SNR message towards Policy even after receiving STR, then this SNR gets responded by Policy with 2001 success instead of expected DIAMETER_UNKNOWN_SESSION_ID result code.	3	22.3.0, 22.2.0, and 22.1.0

Table 4-19 CNC Policy 22.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
34227033	UDR_UMDATA_COMPARE_FLAG not working on PDS	UDR_UMDATA_COMPARE_FLAG is not working on PDS.	3	22.2.0
34225981	OverloadThreshold configurations are overwritten during upgrade	OverloadThreshold configurations are overwritten during upgrade.	3	22.2.0
34317062	SOAP notification schema, Replication failure with Binding service	Replication failure is observed with Binding service.	3	1.15.4
34512052	PCF Upgrade to 22.2.1 fails and causes db replication errors	In GR site the replication was broken because of the mismatch in character set across 2 sites.	3	22.2.1
34374174	Alerts config files moved from Artifacts to Artifacts/Scripts for Orchestration	AlertConfig file is placed under the Artifacts directory instead of the Artifacts/Scripts.	3	22.2.0
34542205	Helm chart discrepancy for Policy and BSF	Update the appVersion in the helm chart of Policy and stub helm chart of Policy ATS.	3	22.1.2

Table 4-19 (Cont.) CNC Policy 22.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
34542257	Remote Subscriber State Variable(SSV) operation are not working in pcrf-core	Remote Subscriber State Variable(SSV) operations are not working in pcrf-core.	3	1.15.4
34542278	MBR Qos values in AAR-I not getting sent in N7 UpdateNotify as MBR/GBR	MBR Qos values in AAR-I are not being sent in N7 UpdateNotify as MBR/GBR.	3	1.15.4
34542581	Unable to update the “capacity” and “load” parameter in the PCF registration profile	Unable to update the “capacity” and “load” parameters in the PCF registration profile as PCF overwrites it with the calculated nfstatus and capacity.	3	1.15.4

Note:

The resolved bugs from CNC Policy Release 22.2.1, 22.2.2, and 22.2.3 are forward ported to Release 22.3.0.

Table 4-20 CNC Policy 22.3.0 ATS Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
34224235	ModelD_BindingHeader ATS Feature Failing with EGW 22.2.0	ATS Test cases for Model D are not executing.	3	22.2.0
34224296	ATS regression failure in initial run	After restart of the system ATS test cases 3GPP_User_Location_Info_Support and PCF_Interface_Timer_Handling are failed in initial run.	3	22.2.1

Table 4-20 (Cont.) CNC Policy 22.3.0 ATS Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
34542303	Proxy entries need to be removed from BSF & PCF ATS product	ocats-policy pod takes longer to start and it is trying to resolve the proxy. These proxies must be removed.	3	22.1.0
34542659	Developer email address need to remove in bsfuser & policyuser profiles	Developer email address need to be removed in policyuser profiles.	3	22.1.0

Note:

The resolved ATS bugs from CNC Policy Release 22.2.1, 22.2.2, and 22.2.3 are forward ported to Release 22.3.0.

4.2.7 NEF Resolved Bugs

NEF Release 22.3.2

There are no resolved bugs in NEF Release 22.3.2.

NEF Release 22.3.0

There are no resolved bugs in NEF Release 22.3.0.

4.2.8 NRF Resolved Bugs

Table 4-21 NRF 22.3.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34896743	NRF 22.2.2 NFSET Feature Returning SetID as All upper case	NRF is sending nf-set id in NF profile in upper case when discovery is sent with nf-set id.	2	22.2.2
34985827	Replication threads crash requires pod restart in OCNRF microservices	If replication threads crash in the microservices, then pod restart is required to reinitialize the threads. Lifecycle management of replication threads is now controlled by Spring Boot framework.	2	22.2.2

Table 4-21 (Cont.) NRF 22.3.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34985618	NF is not moving into Suspended state from Probable-suspended even when HB is stopped and Replication is up.	NF is not moving into suspended state from probable-suspended even when Heartbeat is stopped and replication is up.	2	22.3.0
34880889	In NRF performance for a traffic of approx 38K TPS with CPU utilization beyond L1 level, Overload load level is not getting triggered and alert is not generated	The following REST URIs used for configuration are incorrect: • /nrf/nf-common-component/v1/igw/errorcodesseriesList must be changed to errorcodeserieslist • /nrf/nf-common-component/v1/igw/errorcodesProfiles must be changed to errorcodeprofiles	2	22.4.0
34937707	Certain commands present in NRF rollback procedure from 22.3.1 to 22.2.X needs to be removed and modified from NRF Installation and upgrade guide	Certain commands in NRF rollback process are obsolete and must be removed from the rollback section of Network Repository Function Installation and Upgrade Guide.	3	22.3.1
34985782	During OCNRF DB Resync and DR procedures, some time Auditor threads are crashing	During OCNRF DB Resync and DR procedures, some time Auditor threads are crashing	3	22.3.2
34984630	After approx 54 hr long run subscription pods move in 1/2 state with ERROR as java.lang.OutOfMemory Error	NF subscription pod is experiencing out of memory issue. Thread optimization is required to spawn required threads.	3	22.4.0
34643799	Extract and use User-Agent header as per 29.500	OCNRF is not separating out user-agent header and extract NFtype from user-agent header in Access Token microservice.	3	22.1.0

Table 4-21 (Cont.) NRF 22.3.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34985756	Roaming: OCNRF Needs to relax check of attributes when Roaming is disabled AccessToken and Subscription	Roaming specific attributes are present in the requests even when roaming is disabled. The requests must be processed even if there are roaming specific attributes.	3	22.2.2
34985737	NRF Subscription Forwarding for Subscription Update and Delete is using only 2 sites	NRF subscription forwarding for subscription update and delete is using only first two sites that are configured. OCNRF must consider all NRF sites configured for NRF subscription forwarding for subscription update and delete.	3	22.3.1
34985578	useRemoteDataWhenReplDown attribute description is not correct in the document	useRemoteDataWhenReplDown attribute description does not correctly explain the scenario where this attribute is applied.	3	22.2.2
34985864	OCNRF there is no way to indicate that db replication threads are not running	There is no way to indicate that DB replication threads are not running. Hence, metric and alert are needed for thread cash enhancement.	3	22.2.2
34249952	Add missing Resource/ Verbs for Helm Test to OCNRF ServiceAccount	Missing resource or verbs in service account are leading to permission issues. All the resource or verbs must be added to OCNRF service account in the document.	4	22.2.0

NRF-ATS 22.3.2 Resolved Bugs

Table 4-22 NRF-ATS 22.3.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
34618783	SLF03_discovery_slf_query and Subs03_with_NotifCondition test cases failed during the nightly run	While running SLF03_discovery_slf_query and Subs03_with_NotifCondition test case, exception is seen in ATS POD log which is resulting into test case failure.	2	22.3.1

Table 4-23 NRF 22.3.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
34618783	After NRF rollback done from 22.3.0 GA to 22.2.0 GA, NRF upgrade fails from 22.2.0 GA to 22.3.0 GA	The following upgrade or rollback sequence is failing due to conflicting hpa resources. 22.2.x upgrade to 22.3.0 -> rollback to 22.2.x -> again upgrade to 22.3.0.	2	22.3.0
34693248	NRF R16 ServiceMap feature - Error code 400 for Heartbeat request after Upgrade from 22.2.0 to 22.3.0	Heartbeat Request getting Error code 400 (BAD Request) after upgrade."problemDetails":"{\"title\":\"Bad Request\",\"status\":400,\"detail\":\"JSONInvalid Format\",\"cause\":\"Bad Request\"}"}	3	22.2.0
34693318	EmptyListFeature - Suspended Profiles with Services Suspended are not included in the response.	When the EmptyList feature is enabled, and an NfProfile has its nfStatus as SUSPENDED, along with its services in SUSPENDED state, the profile does not get included in the discovery response.	3	22.1.4

Table 4-24 NRF 22.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
34426848	Incorrect service name available on doc and while configuring incorrect name, IGW accepting it	Incorrect service name available on Rest Specification Guide and while configuring incorrect name, Ingress Gateway accepting it. sbiRoutingErrorActionSets and sbiRoutingErrorCriteriaSets name mentioned in doc are not correct.	3	22.2.0
34205881	DNS record can be stale if deregister request of AMF is not successfully processed by OCNRF	DNS record can be stale if deregister request of AMF is not successfully processed by OCNRF and hence deletion of DNS NAPTR record is not sent towards DNS Server.	3	22.2.0
34541960	EmptyList: Failure occurred before forwarding is not getting considered in case of non-2xx and 200 no profile	EmptyList: Failure that occurred on NRF1 before forwarding to NRF2 is not getting considered in case of non-2xx and 200 no profile response from NRF2. Use-Case- SLF failure 4xx (Except 404) and 5xx Suspended profiles forbidden.	3	22.2.0
34542221	OCNRF sending 415 when GZIP is disabled at OCNRF	OCNRF sending 415 when GZIP is disabled at OCNRF. Instead without gzip encoded response shall be sent.	3	22.1.0
34427105	NRF sends dynamic DNS update to DNS servers but the same records are not seen in nrf-status-data ouput.	Non intended records in cache with similar keys are getting updated with incorrect sync status. On successful removal of records from DNS server, only values are getting removed from cache while cache entry comprising of keys and empty values are still present.	3	22.2.0

Table 4-24 (Cont.) NRF 22.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
34247494	OCNRF Status APIs return local records in Geo-Redundant deployment NRF	Due to software bug, even DB replication is healthy. OCNRF status APIs for NFInstances and Subscription returns only local Records.	3	22.1.0
34542954	NRF Istio-logs contain unexpected dashes	maxLifetime parameter value is lesser than hikariIdleTimeout value.	3	1.15.1
34543030	ATS is failing on the regression test.	Update systemOptions_cleanup.sh script provided as part of ATS for nfAccessTokenOptions and validate other configurations	3	1.15.0
34543117	Not able to view NRF Logging level though able to change it in CONSOLE	Not able to view NRF Logging level though able to change it in CONSOLE.	3	22.2.0
34543152	Notification trigger is not being sent out by auditor pod	Notification trigger is not being sent out by auditor pod for remote record when a SUSPENDED profile is moved to DEREGISTERED state by the profileAudit cycle. Also, the nfStatus in the NfInstances and NfStatusMonitor tables are inconsistent.	3	22.2.0
34468772	NF Discover: SLF Lookup not happen for Suspended NF Profiles	While processing NF Discover Service operation, SLF lookup doesn't happen for Suspended target NF Profiles. This is required for Empty List feature as it works on Suspended NF Profiles.	3	22.1.0
34468871	Supi and Gpsi filter being ignored when slfLookup request is not sent or SLFLookUp didn't result GroupId due to some error	Supi and Gpsi filter being ignored when slfLookup request is not sent or SLFLookUp didn't result GroupId due to some error	3	22.1.0

Table 4-24 (Cont.) NRF 22.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
34251699	EmptyListResponse processing is taking priority ahead of forwarding in NfDiscovery service operation	Suspended forbidden profiles are taking priority than forwarding logic.	3	22.1.0, 22.2.0
34537141	Discovery query not responded correctly with EmptyList feature when simultaneous requests are received	Discovery response for PCF is getting no profiles sometimes while using ATF.	3	22.1.3
34537487	OCNRF Roaming scenarios 2-digit MNC need to converted in Header: 3gpp-sbi-target-apiroot	OCNRF Roaming scenarios 2-digit MNC need to converted in Header: 3gpp-sbi-target-apiroot Right now OCNRF is not appending '0' in 2-digit MNC to make it as 3 digits.	3	22.1.0
34547333	NFServiceList: NFServices and NFServiceList both are not working vice-versa randomly when Patch is applied on Service level attribute.	NFServiceList: NFServices and NFServiceList both are not working vice-versa randomly when Patch is applied on Service level attribute.	3	22.2.0
34549484	NRF: Updates Requested In CSAR MF File	Updates requested In CSAR MF File has special characters such as spaces and tabs.	3	22.2.0
34554642	During upgrade, 25% Max unavailability is not taking effect	During Rolling Upgrade it is observed that even if maxUnavailable is configured as 25%, all expect 1 pod goes down during upgrade. This will result in traffic loss.	3	22.1.4
34082721	Continues Error Log in Perf-Info Pod for Jaeger Tracing Issue	In the perf-info service, the mentioned error logs are observed periodically (in every 30 seconds) due to jaeger. There is no functionality of perf-info impacted.	4	22.1.0
34537375	NF Subscription: CreationTimeStamp getting updated during Duplicate Subscription processing	NF Subscription: CreationTimeStamp getting updated during Duplicate Subscription processing.	4	22.1.0

Table 4-24 (Cont.) NRF 22.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
34347713	"DNS_NAPTR_OPTIONS" deletion step missing in User Guide during rollback from 22.2 to 22.1.*	"DNS_NAPTR_OPTIONS" deletion step missing in User Guide during rollback from 22.2 to 22.1.*.	4	22.2.0
34394563	NRF NF_Register screening rules needs precision in our documentation	NRF NF_Register screening rules needs precision in our documentation. Add detailed description for each screening rule parameters.	4	22.3.0

Note:

Resolved bugs from 22.1.4 and 22.2.1 have been forward ported to Release 22.3.0.

4.2.9 NSSF Resolved Bugs

NSSF 22.3.2 Resolved Bugs

There are no resolved bugs in this release.

Table 4-25 NSSF 22.3.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34633548	Issue with common config server which is used for run time log level update while upgrading from 22.2.1 to 22.3.0	During NSSF upgrade from 22.2.1 to 22.3.0, the Upgrade hook job of the Common Config Server is not getting instantiated.	3	22.3.0
34646259	NSSF Upgrade from 22.2.1 to 22.3.0 fails: "Duplicate column name 'mcc'"	NSSF upgrade has an issue when a scenario of 22.2.x→22.3 is done. In a situation when the upgrade is done post a roll back the issue of a Table column addition is being observed.	3	22.3.0
34646261	NSSF rejects NRF notification with 404 for auto subsribctions by NRF Client	NSSF does not support notifications for autosubscriptions. NSSF must disable autosubscriptions at NRF.	3	22.3.0

Table 4-25 (Cont.) NSSF 22.3.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34572732	Wrong username mentioned on Grant cmd for NSSF installation document , while executing same getting ERROR 1410 (42000)	Sample usernames of the grant commands are not in sync in the document. Must ensure to use the same usernames throughout the document.	4	22.3.0
34646263	NSSF Documentation: Update the Installation and Upgrade guide for the Oauth Configuration	It is required to add steps for Oauth configuration in the installation guide.	4	22.3.0

Table 4-26 NSSF 22.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34206366	GUI for log level is not as per design.	CNCC GUI to configure the log level is not working for Application logs. Currently, the application level log is being updated by the GUI button for the root log level.	3	22.1.0

4.2.10 NWDAF Resolved Bugs

NWDAF 22.0.0 Resolved Bugs

There are no resolved bugs.

4.2.11 SCP Resolved Bugs

Table 4-27 SCP 22.3.4 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34927431	SCP does not match routing rule when 3gpp-sbi-target-apiroot contains capital letters	SCP was not making FQDN case insensitive while matching FQDN from NF profile with incoming request FQDN in 3ggp-sbi-target-apiroot.	3	22.3.0
34919781	Enhanced_NF_Status_Processing_UNDISCOVERABLE scenario failure	Configuration clean up was missing in one the scenarios causing intermittent failure.	3	22.3.2
34973017	SCP CSAR file Definitions/ocscp.yaml file has invalid yaml	Indentation changes are required in the CSAR package.	3	22.3.0

Table 4-28 SCP 22.3.3 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34883536	content-length=0 is being added by SCP in the 204 No Content response	SCP adds content-length as 0 in the response that SCP relays on the downstream path.	2	22.3.2
34879008	NF Discovery for R16 Model-D Uses CUSTOM_ORACLE_SCP in User-agent header instead of SCP	NF Discovery for R16 Model D uses CUSTOM_ORACLE_SCP instead of SCP in the User-Agent header.	3	22.3.2

Table 4-29 SCP 22.3.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34766366	Upgrading SCP 22.2.1 to 22.3.1 failing on POST-upgrade config pods	The upgrade from SCP 22.2.1 to 22.3.1 is failing due to timing and slowness of pods coming up. It is observed on the ASM setup.	3	22.3.1
34815356	Alert_SCPEgressTrafficRoutedWithoutRateLimitTreatment testcase is failing	Fixed cleanup of the scenario causing the failure in Alert_SCPEgressTrafficRoutedWithoutRateLimitTreatment testcase.	4	22.3.1
34797551	Alert_SCPEgressTrafficRateExceededConfiguredLimit feature failing in individual run	The SCPEgressTrafficRateExceededConfiguredLimit alert was failing due to configuration step missing in testcase.	4	22.3.1

Table 4-30 SCP 22.3.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34697102	Inter SCP notification routing not working when request URI is missing service name	Inter SCP notification routing is not working when request URI is missing service name and was taking forward route to producer NF.	2	22.1.2
34701790	SCP Frequently Subscribing and Unsubscribing to NRF over TLS	SCP is picking up incorrect port for https and thus detecting change in NRF ipendpoint for callback URI. This was causing frequent subscription and unsubscription to NRF over TLS.	2	22.1.2

Table 4-30 (Cont.) SCP 22.3.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34614606	TrafficFeed feature throws indexOutOfBoundException on getting producerFqdn when 3gpp-sbi-target-apiroot header value does not have port Info	The TrafficFeed feature throws indexOutOfBoundException on getting producerFqdn when the 3gpp-sbi-target-apiroot header value does not have port information.	3	22.3.0
34641690	"ocscp_notification_foreign_nf_locality_unserved" metric is not decrementing	"ocscp_notification_foreign_nf_locality_unserved" is pegged when a NF register with locality not served by any SCP but is not cleared when NF deregister.	3	22.1.2
34617666	scp_vnfd.mf" file Corrections Requested in SCP	The "scp_vnfd.mf" file is corrected through reformatting.	4	22.3.0

Table 4-31 SCP 22.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34235146	SCP would not be able to recover the connection with NRF in case of failure	SCP was not able to create HTTPS connection again if any existing connection is terminated.	2	22.2.0
34298705	An exception occurred on SCP after applying mediation rules to the nnrf-nfm service	nullpointer exception was observed while applying trigger point configuration for nnrf-nfm service.	2	22.2.0
34335985	SCP is not processing new SUPI range	The SCP Notification module was unable to process supi range addition to the existing NF profiles when the number of profiles are high.	2	1.15.3
34212938	Observed worker pod restart during the performance run on ASM setup with hybrid traffic model	SCP-worker pods restarted during performance run with the hybrid traffic model.	2	22.1.2
34455997	Discovery failing in Model-D inter plmn request	SCP was failing to route to discovery request to NRF in case of inter-plmn request and sending 404 response code back.	2	22.2.0

Table 4-31 (Cont.) SCP 22.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34398036	Access token request routing not working via SCP	SCP was not able to route access token request with content-type as application/x-www-form-urlencoded. Enabled support for content-type as application/x-www-form-urlencoded on SCP.	2	22.2.0
34267593	404 returned on re-running a Model-C inter plmn request	SCP was sending 404 response code on Model-C interplmn request due to via header decoding issue in request.	2	22.2.0
34330089	SCP displays inconsistent behavior by applying deleted trigger rules for mediation	SCP was retaining some deleted trigger rules in cache and applying them to send request to mediation service.	2	22.2.0
34301561	Mediation is not applied correctly as per trigger point groupId configuration	SCP was not routing request to mediation service correctly as per groupId configured in trigger point configuration.	2	22.2.0
34275009	Update ATS FTs for FQDNs to address DNS query failure	DNSSRV ATS test cases are modified for all FQDNs of various NF profiles to be of the same pattern that matches searches block added in the alternate-resolution microservice deployment specification. Otherwise, the resolution of such FQDNs takes more time resulting in failure of FTs on various setups.	3	22.1.1
34335935	ATS multiple features were failing due to "TypeError: the JSON object must be str"	Multiple features of ATS were failing due to "TypeError: the JSON object must be str" and the ATS FW Step was not picking up the correct data files.	3	22.2.0
34335955	SCP is not able to route NF notification request from NRF with https signaling port	The SCP-worker was not forwarding notification requests received with https port to the notification module.	3	22.1.2
34423274	Exception in creating Interplmn routing rule when capacity is not provided in NFProfile	SCP required capacity in the SEPP NF Profile to create routing rules for SEPP NF.	3	22.1.2

Table 4-31 (Cont.) SCP 22.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34423296	SEPP Profile is removed from NFProfiles when SeppInterPlmnInfo is removed	Removal of SEPP profile was resulting in SeppInterPlmnInfo configuration.	3	22.1.2
34472956	504 - Destination Client Response TimeOut errors	Notification pod memory was increasing and notification processing was taking more time resulting in 504 timeout. Issue with notification memory build up is fixed to resolve the issue.	3	22.1.2
34477476	SCP is not correctly matching plmn with sbi request when 2 digits mnc is configured in SCP Profile	SCP was unable to match the mnc in incoming request if 2 digits mnc is configured in SCP Profile. Fixed to add padding to 2 digits mnc before comparison with incoming request.	3	22.1.2
34499261	Egress Rate Limit feature throwing 503's and Circuit Breaking triggered	Circuit breaking was getting triggered in case of egress rate limiting. Pending request count was not decremented correctly in case of egress rate limit resulting into the issue. code fixed for same.	3	22.2.1
34423315	SCP is not routing based on 3gpp sbi apiroot rather using interplmnhost for routing	SCP was routing initial request based on interplmn host in NF Profile instead of 3gpp-sbi-target-apiroot header received in case of interplmn fqdn in request.	3	22.1.2
34423339	Update Alert expression for db fetch failures and typo in memory alerts	Updated the description of SCPNotificationPodMemoryUsage and SCPWorkerPodMemoryUsage alerts in the SCP User Guide.	3	22.1.2
34508046	SCP deletes part of the URI for notification request	SCP was removing prefix before service name in the request URI even when request is received with callback header.	3	22.1.2
34513171	SCP not removing de-registered EIR NF	SCP was failing with exception to match the NFType for 5G_EIR in notification, audit, and subscription.	3	22.1.2

Table 4-31 (Cont.) SCP 22.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34302670	ReidrectUrl should be optional when applying DISCARD Action Policy with 4xx or 5xx response code	SCP was authorizing to provide redirect URL when applying message discard policy based on priority for 4xx and 5xx response code.	3	1.15.4
34275033	SCP is not rerouting when 307 response with retry-after header is received from producer NF	SCP was not alternate routing when retry-after header is received with 307 response with producer NF.	3	1.15.3
34499058	Remaining capacity of the wait queue for notification service doesn't become zero even with pod restarts	SCP was processing all the profiles again after notification pod restart.	3	22.1.0
34355852	Traffic loss observed while performing the nrf-proxy restart	Some traffic loss was observed during nrf-proxy pod restart during the performance run.	3	22.1.1
34348067	Observed 100% CPU utilization of worker pod in case of 230K TPS run on a non ASM setup	SCP-worker pod was reaching 100% CPU during the performance run.	3	22.1.1
34317658	SCP worker init container goes into error when HTTPS is enabled, as log level of worker set to DEBUG and if gets changed to INFO it gets deployed	SCP-worker pod was unable to come up when deployed with debug logs and https enabled.	3	22.1.2
34293162	PlmnSeppMapping rules consider scheme as https when value of https field in SEPPInfo is empty	SCP was taking default scheme as https when https field is provided with empty value in SeppInterPlmnInfo configuration.	3	22.1.2
34134466	SCP-SEPP_FT: SCP adds incorrect User-Agent while sending discovery towards NRF	SCP was adding default jetty user-agent header while sending delegated discovery request to NRF.	3	22.1.2
34093853	SCP is responding with incorrect location while performing alternate route of notification request with discovery headers	SCP was replacing location header in response with 3gpp-sbi-target-apiroot even when it is alternate routed to different producer for notification request with discovery headers.	3	22.1.1
34030648	NF re-selection not working for intra plmn scenario	SCP was not selecting correct NF profile for alternate route when request is received with incorrect port in 3gpp-sbi-target-apiroot.	3	22.1.0

Table 4-31 (Cont.) SCP 22.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34449323	Incorrect CPU and memory values in the deployment yaml	Default request values of CPU and Memory in the deployment file of mediation service was incorrect.	3	22.2.0
34449321	Duplicate key in env variables in the deployment yaml	Duplicate keys in the mediation deployment file was removed.	3	22.2.0
34449320	Duplicate ports are present in the deployment yaml when deployed with default values	Duplicate ports in the mediation deployment file was removed.	3	22.2.0
34349589	Ocscp_mediation_http_rx_total is pegged with incorrect response code in case of responseEgress	The ocscp_mediation_http_rx_total metric is pegged with incorrect response code, so a note has to be added in the SCP User Guide indicating that the response is received by SCP from Mediation.	3	22.2.0
34355892	Mediation metrics are not getting pegged when mediation pod reaches 7vcpu during performance run though RULE_METRICS_ENABLE is set to true	Metrics were not pegged when CPU utilization on scp-worker reaches the limit. Optimization done on SCP to reduce the CPU utilization during the performance run.	3	22.2.0
34355882	Observed that ocsp_response_code 503 is returned from mediation to worker during the performance run	SCP was generating intermittent 503 errors while trying to send traffic to mediation service during the performance run.	3	22.2.0
34355857	SCP Mediation processing time unit needs to be fixed in dashboard	Units for metric ocscp_mediation_upstream_service_time_ms_total was not correct on the Grafana dashboard.	3	22.2.0
34349572	SCP deployment file does not contain the parameter to enable Mediation service metrics	Parameter to enable the Mediation service metrics was missing in the SCP deployment file.	3	22.2.0
34293130	Appversion is not correct in SCP ATS Helm charts	App version was set to 1.0 in Helm charts instead of current release.	4	22.1.2
34311844	The SCPInstanceDown alert has missing alert name among its labels	A few alerts were missing the alert name label.	4	22.2.0

Table 4-31 (Cont.) SCP 22.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34349564	Inconsistency observed in the ociwf_med_active_rule_count metric with implementation	The description of ociwf_med_active_rule_count metric represents the total number of rules which can be invoked for a particular message, however, there is no message information in the dimension of this metrics.	4	22.2.0
34342262	Alternate routing using static configuration has Mediation topic related information	The "Support for Alternate Routing Using Static Configuration" section in the SCP User Guide has be updated by removing the mediationService parameter reference.	4	22.2.0
34307580	Correct the name of the Mediation metric (ocscp_mediation_upstream_service_time_ms) in the SCP User Guide	The name of the Mediation metric, ocscp_mediation_upstream_service_time_ms, is replaced with "ocscp_mediation_upstream_service_time_ms_total" in the SCP User Guide.	4	22.2.0
34128219	SCP-NRF Interactions during startup and runtime need to be captured in SCP User Guide	Capture the SCP and NRF interaction in the User Guide. Additionally, capture what is the nfStatusNotificationUri used by SCP.	4	22.1.1
34030663	SCP compliance matrix 29500 6.10.8.2 need be updated from FC to PC	As per SCP compliance matrix, the 3GPP 29500 section 6.10.8.2 has been marked as "FC", whereas the error response is not fully compliant.	4	22.1.0
34274814	Feature and data files are not copied from product folder to custom folders	A few feature and data files were missing in the custom folder but were present in the product folder.	4	22.2.0
34336011	SCP Alert name mismatch in User guide with respect to Alertrules yaml file	SCP User Guide is updated to match the alert names.	4	1.15.3
34498881	"scp_vnfd.mf" file Corrections Requested	vnf_release_data_time is changed to vnf_release_date_time and a blank space removed from the scp_vnfd.mf file in csar package.	4	22.2.1
34423364	END statment missing in MIB TC file	Updated MIB files to add END statement and some missing labels.	4	22.1.2

Table 4-31 (Cont.) SCP 22.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34336302	unquoted alertnames defined within SCP_Alertrules.yaml	While performing deployment validation tests, a few discrepancies were observed in the configuration of a small set of alerts that were defined without double quotes (" ") within the SCP_Alertrules.yaml file.	4	22.1.2
34336310	RateLimitingReleaseR16 feature cleanup scenario is failing	The RateLimitingReleaseR16 feature was failing due to some inessential steps used for cleaning up this feature.	4	22.2.0
34274897	503 response error log shows unknown ID in the Body field	SCP-worker logs were showing reference ID in 503 error responses.	4	1.15.0

Note:

Resolved bugs from 22.1.3 and 22.2.2 have been forward ported to Release 22.3.0.

4.2.12 SEPP Resolved Bugs

Table 4-32 SEPP 22.3.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34533995	RemoteSEPP Delete REST API at config mgr returns success incase underlying failures	Deleting the RemoteSEPP REST API at the config mgr returns success in case of failure also. RemoteSEPP remains in database even after running the delete command. This occurs randomly and not for all the cases.	4	22.3.0
34892299	Latency metric corrections required in user guide	Some of the metrics dimensions are different in user guide and code. Security Edge Protection Proxy User Guide has been updated to make it consistent.	4	22.4.0

Table 4-32 (Cont.) SEPP 22.3.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34745796	SEPP-PERF: Some correction require in Grafana graph heading showing in milli second(ms) and value in traffic instead of second(s)	Some correction is required in the Grafana graph heading, which is showing values in milliseconds instead of seconds. 1. CN32F processing time graph heading showing the values in msec. 2. PN32F processing time graph heading showing the values in ms and value of min, max, and, avg showing in Million. 3. IGW processing time graph heading showing the values in ms. 4. EGW processing time graph heading showing the values in ms.	4	22.3.0
34805799	SEPP helm test failing	When the release is deployed with any name other than the ocsepp-release, helm test is failing and not giving the expected output. The code has been updated to remove this dependency and release name has been hardcoded in helm test.	4	22.3.0

Table 4-33 SEPP 22.3.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34598891	Incorrect seppMetricDashboard-promha.json delivered as a part of csar package,	seppMetricDashboard-promha.json was incorrect. Updated it to correct values.	2	22.3.0
34569426	kubernetes_name parameter should be a part of custom yaml file.	Some of the parameters were part of internal values.yaml file. Move them to custom-values.yaml file. • Exposed Timeout of IGW and EGW in custom-values.yaml • exposed tag_namespace and other prometheus variables that can be set on the basis of OCCNE version	3	22.3.0

Table 4-33 (Cont.) SEPP 22.3.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34623009	Roaming-hub custom-values is missing from SEPP 22.3.0 CSAR package	roaming-hub custom-values.yaml file was missing from CSAR package. This file is used to install Roaming-hub.	3	22.3.0
34698167	Mediation is not updating path in trans-context when applied on PATH header	Mediation is not updating path in trans-context when mediation is applied on values of PATH header.	3	22.3.0
34657934	Dimensions & metrics missing from user guide	The latency metrics and dimensions to be added to SEPP User guide. The following metrics to be removed from SEPP User guide: ocsepp_pn32f_latency_total and ocsepp_cn32f_latency_total	4	22.3.0
34534058	Handshake alert is not getting cleared in some error scenarios	Handshake failure alert raised is not getting cleared when the successful handshake is completed in some of the scenarios: • when the handshake failure is sue to incorrect FQDN • When the handshake failure is due to incorrect plmn	4	22.3.0

Table 4-34 SEPP 22.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34374404	Egress Gateway peer, peerset, routes configuration parameter in custom yaml	PLMN Egress Gateway route configuration parameters were missing from custom-values.yaml. Added the parameters in the ocsepp_custom-values_<version>.yaml file, so that it can be configured as per the user network.	3	22.2.0

Table 4-34 (Cont.) SEPP 22.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34374452	SEPP-COM-xx-ERROR-0103 is not observed when n32c pods have been scaled down	When N32c service was unreachable, a timeout error message is generated. Previously, there was no method to identify the real cause of the timeout. Added specific conditions and details in the error cause section to mention that the service is unreachable.	4	22.2.0
34374461	Complete information is not displayed for SEPP-COM-xx-ERROR-0102	In some of the SEPP-generated errors, java-related internal errors were getting filled as an Error reason. Updated the code to display user-friendly error reasons which make it easy for debugging.	4	22.2.0
34364488	The proper error should be displayed when the name field is missing from the PUT request	In some of the SEPP-generated errors, java-related internal errors were getting filled in Error cause. Updated the code to display user-friendly error causes which makes it easy for debugging.	4	22.2.0
34351407	Invalid parameters were observed in the response of the PATCH request for remotesepp configuration	Due to an incorrect port getting set in the PATCH request, the PATCH response always displayed port=0 along with the updated parameter. Updated the code and now, only the updated parameter value will get displayed in the response object.	4	22.2.0
34331825	Remotesepp PUT request accepts a name as blank	Added code to check if the name is empty in *RoamingPartnerDTO*, then use the same namefrom path parameter.	4	22.2.0
34331841	The proper error should be displayed when seppFQDN is set as blank in PUT request for remotesepp configuration	Updated the response error cause and added Empty check for SeppFQDN in PUT remotesepp request.	4	22.2.0
34331869	In PATCH request for remotesepp configuration if plmmlist is set as blank 200 OK is returned.	Added a check to have plmn id list mandatory while configuring RemoteSepp. Proper error handling is added to the code and the error cause is set to descriptive error.	4	22.2.0

Table 4-34 (Cont.) SEPP 22.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34311321	Remoteseppset configuration returns plmnIdList as blank when configured remotesepp is set as secondary	The issue was PLMNID list in RemoteSeppSet was getting picked up from Primary RemoteSepp even when primary remote sepp is not even associated in RemoteSepp Set. Added a check to pick up the PLMNID list for RemoteSeppSet from Primary or Secondary or Tertiary RemoteSepp, whichever is configured.	3	22.2.0
34249854	Remote Set form allows security capability other than TLS/PRINS	Created an enum of TLS and PRINS. With this change, only allowed values for TLS or TLS+PRINS.	4	22.2.0
34235805	For alert, SEPPPodMemoryUsageAlert summary doesn't display proper information.	Corrected namespace label as namespace: ' {{ $labels.namespace}} '. Removed nfinstanceId from both CPU and Memory usage alerts.	4	22.2.0
34298510	Corrections are needed with regard to the metrics in the SEPP user guide	Some of the egress gateway and ingress gateway metrics were placed in the incorrect section in the User guide. Added the metrics to their respective sections.	4	22.2.0
34263214	Corrections needed in SEPP REST SPECIFICATION	There are a few error codes that need to be corrected in the REST Specification guide. Correct details are added for these error codes. • SEPP-COM-xx-ERROR-0101 • SEPP-COM-xx-ERROR-0009 • SEPP-COM-xx-ERROR-0023 • SEPP-COM-xx-ERROR-0003 • SEPP-COM-xx-ERROR-0010	4	22.2.0

Note:

Resolved bugs from 22.2.1 have been forward ported to Release 22.3.0.

4.2.13 UDR Resolved Bugs

Table 4-35 UDR 22.3.4 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34956225	SLF 22.3.3/ATS 22.3.4 Regression Pipeline failed	SLF ATS regression pipeline is failed due to Kubernetes timeout error.	2	22.3.3

Table 4-36 UDR ATS 22.3.4 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34799306	SLF-ATS 22.3.3 SLF_Subscriber_Data_Dump feature is failing	If the lost+found directory is missing on the customer site, ATS would fail. As a fix, ATS will now look only for the exported files.	2	22.3.3
34845797	SLF_Subscriber_Data_Dump.SLF_WEEKLY_SUBS_DUMP_CLEANUP_14 scenario failed	Export tool deployment related changes are made in the custom values yaml file. For more information, see Running UDR Test Cases using ATS in *Oracle Communications Cloud Native Core Automated Testing Suite Guide* .	2	22.3.3

Table 4-37 UDR ATS 22.3.3 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34740405	SLF ATS 22.3.2: SLF_Config_Import_Export.feature failures	Regression test cases is failed in SLF ATS 22.3.2 release.	2	22.3.3

Table 4-38 UDR 22.3.3 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34691030	SLF 22.3.1/ ProvGW 22.3.0 upgrade failed	SLF 22.3.1 and ProvgGW 22.3.0 upgrade failed with the error related to hpa.yaml file.	2	22.3.1
34607301	messageTimestamp format is incorrect for provgw-provgw-config pods	Few of the pods contain the wrong message timestamp format in their logs.	3	22.2.1

Table 4-38 (Cont.) UDR 22.3.3 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34647426	Provisioning update for a subscriber key does not replace but add them to its profile	SOAP update query is performed in order to replace some keys for a particular subscriber, but using the same query in ProvGw, some keys are not replaced but are added.	3	22.2.0
34507725	Get Request Fails for VSA when UmData fields are removed from SM-DATA	When UmData fields are removed from SM-DATA, Get request fails for VSA.	3	22.2.0
34502997	DELETE VSA for NSSSAI is not deleting the subscriber	If the VSA is configured at Single - Network Slice Selection Assistance Information (S-NSSSAI), the subscriber is not deleted.	3	22.2.0
34613484	SLF group provisioning/ mapping fails on SLR/UDR in combined mode	Not able to map the subscriber IMSI with SLF group created when using SLF in the conversed mode. SLF APIs reports 'Key already exist' for this subscriber.	3	22.2.0
34558113	Error Description is incorrect for VSA PATCH Request	VSA PATCH request has incorrect error description.	3	22.2.0
34646666	ATS New Feature - Subscriber Activity logging failed in lab	ATS test case is failed for the subscriber Activity logging feature.	3	22.3.1

Table 4-39 UDR 22.3.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34614383	Updates Requested In CSAR MF File	In the ProvGW and UDR manifest files, the entire blank line delimiter at the end of the meta data section is removed. The feedback was to remove only the whitespace and not to remove the line completely.	3	22.3.0
34614544	Missing double quotes in ProvGw Alerts yaml file	Double quote is missing in line 114 of the ProvGw_Alerts.yaml file.	3	22.3.0

Table 4-40 UDR 22.3.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34559281	nrf-client-nfmanagement pre upgrade fails during 22.2.1 to 22.3.0 upgrade	When upgrading from 22.2.x to 22.3.0 the nrf-client-nfmanagement pre upgrade fails due to issue in the charts.	3	22.3.0

Table 4-41 UDR 22.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34375220	SLF Nu-drservice restarted due to OOM kill exit code 137	SLF nu-drservice pods are getting restarted due to high CPU usage with OOM killed exit code 137.	2	22.2.0
34375332	Provisioning requests failure on ingress-prov due to 500 error after 800 TPS	Provisioning requests failure on ingress-prov due to error (code 500) when traffic rate is more than 800 TPS .	2	22.2.0
34464889	Subscriber Object is missing in Notification from UDR	Subscriber Object is missing in VSA when notification is sent from UDR.	2	22.2.0
34464455	Policy Data is not getting updated in UDR as per the PUT Payload	PCF is not getting updated in UDR as per the PUT Payload when provisioned data is updated using PUT Operation.	2	22.2.0
34444982	UDR is giving successful response to GET request with non-existing dnn & snssai query filters in SM data.	When query user is enabled and both SNSSAI & DNN are included in GET request, it should fail for non-existing filters but UDR gives a successful response to GET request. This occurs when both dnn & snssai parameters are true in PCF and values are non-existing.	2	22.2.0
34403161	UDR is not sending notification to PCF for 4g policy data change	UDR is not sending notification to PCF for Policy data change.	2	22.2.0
34444886	UDR is not accepting SNSSAI value parameter as per specification	SM policy data in UDR is provisioned with SNSSAI filter values. But when SM create is initiated, PCF is rejecting the request with 400 Bad Request.	3	22.2.0

Table 4-41 (Cont.) UDR 22.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34426733	By-default custom yaml apiVersionInUri mentioned as V1 and apiFullVersion as 2.1.0.alpha-3	The default custom_value.yaml mentions apiVersionInUri as V1 and apiFullVersion as 2.1.0.alpha-3.	3	22.2.0
34403382	PATCH Operation is failing for 4g and 5G Policy Data	Patch operation is failing with reason "Invalid Content request Data Supplied".	3	22.2.0
34204095	overloadLevelThreshold is set to empty array when performed upgrade from 22.1.0 to 22.2.0	When performing upgrade from UDR 22.1.0 to 22.2.0, the overloadLevelThreshold value is set to JSON empty array [].	3	22.1.0
34375265	Subscribers are not auto-created for SOAP subscriber profile update requests	SOAP operation to update a subscriber profile must automatically create the subscriber when autocreate flag is set to true.	3	22.2.0
34375054	Provisioning update for a subscriber key does not replace but add it to its profile	Subscriber keys are added to the existing subscriber keys instead of replacing with the key in the payload.	3	22.2.0
34375019	Bulk import tool records 'All records success' for PATCH operations when there are failures	For patch operations on bulk import when there are failures the failed keys are not getting added to the list due to which bulk import records as 'All Record Success'	3	22.2.0
34372032	Extra BillingDay field is added to Subscriber Profile when provisioning using bulkimport	When creating subscriber profile by bulk import tool, UDR allocates the BillingDay field with value equal to 1 automatically, when the query does not have this field set.	3	22.2.0
34371971	Addition of new metric dimensions for ProvGw SOAP requests	The metric provgw_soap_requests_received_total does not have the labels for METHOD to segregate the requests.	3	22.2.0
34184627	"udr-deploy-performance" deployment not getting removed when UDR uninstalled successfully	When UDR is uninstalled successfully, "udr-deploy-performance" deployment is not getting removed. This is a cluster issue.	4	22.1.0

> **Note:**
>
> Resolved bugs from 22.1.2 and 22.2.1 have been forward ported to Release 22.3.0.

4.3 Known Bug List

Known Bugs tables list the known bugs and associated Customer Impact Statements. This information is provided for information purposes only.

4.3.1 BSF Known Bugs

BSF 22.3.4 Known Bugs

There are no new known bugs in this release. For existing known bugs, see Table 4-42 .

BSF 22.3.2 Known Bugs

There are no new known bugs in this release. For existing known bugs, see Table 4-42 .

Table 4-42 BSF 22.3.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
34536385	BSF returning incorrect PCF binding when querying with S-NSSAI	When doing a discovery of pcfBinding with the query parameters, the IPv4 Addr, supi, gpsi, dnn, and snssai, that do not match the snssai registered in the pcfBinding, the pcfBinding is returned instead of a 204 NO CONTENT.	NF service consumers get incorrect binding information when querying with S-NSSAI. Workaround: None	3	1.11.0

> **Note:**
>
> The known bugs from BSF Release 22.2.1 and 22.2.3 are forward ported to Release 22.3.0.

4.3.2 DBTier Known Bugs

DBTier Release 22.3.4

There are no known bugs.

DBTier Release 22.3.3

There are no known bugs.

DBTier Release 22.3.2

There are no known bugs.

DBTier Release 22.3.1

There are no known bugs.

DBTier Release 22.3.0

There are no known bugs.

4.3.3 CNC Console Known Bugs

Release 22.3.2

There are no known bugs in this release.

Release 22.3.1

There are no known bugs in this release.

Release 22.3.0

There are no known bugs in this release.

4.3.4 CDCS Known Bugs

CDCS Release 22.3.1

There are no known bugs in CDCS Release 22.3.1.

Table 4-43 CDCS 22.3.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
34501854	Error upgrading CDCS from 22.2 to 22.3	Upgrading CDCS throws a network connectivity related error.	Customer impact is considered to be low as the error is intermittent and occurs only during certain conditions on the VMware environment. **Workaround**: NA	3	22.2.0

4.3.5 CNE Known Bugs

CNE 22.3.3 Known Bugs

There are no new known bugs in this release.

CNE 22.3.1 Known Bugs

There are no new known bugs in this release.

Table 4-44 CNE 22.3.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
33789640	OpenStack- OCCNE install adds default security group on active LBVM	Openstack default security group is added every time an external IP address is present in the active lbvm machine, along with the security group created for its local interface.	Customer impact depends on the security rules present in the user's default security group. If the user's default security group is restrictive, then the OC-CNE load balancers may not be able to provide service for LoadBalancer services. If the default security group is more permissive, then LoadBalancer services will not be affected. **Workaround**: Contact Oracle customer support for manual procedure.	3	1.9.1 22.1.0

OSO Release 22.3.2

There are no known bugs.

OSO Release 22.3.1

There are no known bugs.

OSO Release 22.3.0

There are no known bugs.

4.3.6 CNC Policy Known Bugs

CNC Policy 22.3.4 Known Bugs

There are no new known bugs in this release. The known bugs from the previous CNC Policy Release 22.3.x are forward ported to Release 22.3.4.

Table 4-45 CNC Policy 22.3.3 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
34693343	race condition encountered in UDR when ims and internet subscription happens together	PCF is sending two subscriptions to UDR when IMS and internet session initiate simultaneously. UDR generates two subscription IDs and sends back to PCF. Intermittently, PCF isn't merging both and store them as a single entry in its database (two entries are created). PCF should send a delete subscription message for one of the subscription ID which is not being triggered.	Stale UDR subscription gets created during the race condition. Workaround: No software workaround. Manual cleanup is possible.	3	22.3.0
34816737	PDS table entries are removed right after upgrade is completed and PCRF-CORE returning 404_NOT FOUND instead of 200 OK	When the upgrade is performed from 22.2.0, the PDS entries created for Gx core sessions are deleted for both the PDS tables causing upgrade scenario failure.	PDS data related to Gx sessions get deleted post upgrade. Workaround: NA	3	22.3.2

The known bugs from the previous CNC Policy Release 22.3.x are forward ported to Release 22.3.3.

Table 4-46 CNC Policy 22.3.2 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
34708976	UE-Subscriber-Activity-Logging: AMF On-Demand-Disc SR, CR not logged at nrf-client and egress	NRF Client does not support Subscriber Logging.	AMF On-Demand-Discovery Server Request and Client Request not logged at nrf-client and Egress Gateway in Subscriber log. Workaround: None	3	22.3.2
34747781	PCF AM UI error: Query user is enabled on GUI but internal configuration shows otherwise	On AM create, on fresh install, configuration for Query user on PCF AM shows as enabled, but internal configuration shows otherwise and it doesn't query the user from PDS.	Incorrect information seen in GUI at first launch. Workaround: Turn off and on flag on UI to sync up config with GUI	3	22.3.2
34746704	UE Subscriber Logging - Subscriber Log at EGW have carriage return in the logs for n1n2-transfer	Subscriber Log at EGW have carriage return(\r) in the logs for n1n2-transfer	None Workaround: None	3	22.3.2
34746900	UE Subscriber Logging - Subscriber Activity Log at IGW not appearing for N1 Notifications	Custom Value files have a typo in the key because of which filters for n1_message_notify were not applied	Subscriber Activity Log at Ingress Gateway not appearing for N1 Notification. Workaround: In CustomValues.yaml change "SubLog" to "subLog" under filters for n1_message_notify. ingress-gateway->routesConfig before upgrade or install.	3	22.3.2

Table 4-46 (Cont.) CNC Policy 22.3.2 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
34746922	UE-Subscriber-Activity-Logging: marker-log not seen for second-fragment transfer request	Subscriber Activity Logs will not work for second-fragment transfer request	Subscriber Activity Logs will not work for second-fragment transfer request. Workaround: None	3	22.3.2
34727304	UE-Subscriber-Activity-Logging: marker-log not seen for second-fragment transfer request	NRF Client does not support Subscriber Logging.	UE Fragmented Message Transfers messages not logged in subscriber log. Workaround: None.	3	22.3.2
34536350	STR Returned with Diameter Unknown Session ID-5002	During the call flow involving CCR-U/T initiated ASR and corresponding STR, if the STR is received on a different pod where CCR-U/T and ASR was not processed, the STR message is responded with 5002 DIAMETER_UNKNOWN_SESSION_ID by pcrf-core.	Call failure reported in overall performance output. Workaround: None	3	22.2.0
34645290	wrong policy decision (user with Quota)	Pcrf-core responds to CCA-I with usage Monitoring AVPs even when subscriber has provisioned quota and Blockly present but no grant action.	Unexpected quota grant occurs during UsageMon activation. Workaround: Disable the Monitoring Key with a blockly in policy project	3	22.2.2

Table 4-46 (Cont.) CNC Policy 22.3.2 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
34644483	PCF behavior on CHF selection when CHF uses pattern while Registration	Pcrf-core responds to CCA-I with usage Monitoring AVPs even when subscriber has provisioned quota and Blockly present but no grant action.	multiple CHF profiles restrict operators to operate with range provisioned. Workaround: CHF profile should be configured with Range if multiple profiles are being used.	3	22.1.0

Table 4-47 CNC Policy 22.3.1 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
34593628	UE-PCF responding to POST create request with 200 OK	Abnormal behavior with UE-PCF response to "POST /npcf-ue-policy-control/v1/policies", with 200 OK instead of 201 CREATED or 4xx/5xx. UE svc then still tried to subscribe to that IMSI - getting 403 response.	A unexpected response is sent when AMF is down. Workaround: None	3	22.2.3

Table 4-47 (Cont.) CNC Policy 22.3.1 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
34536350	STR Returned with Diameter Unknown Session ID-5002	During the call flow involving CCR-U/T initiated ASR and correspondin g STR, if the STR is received on a different pod where CCR-U/T and ASR was not processed, the STR message is responded with 5002 DIAMETER_ UNKNOWN_ SESSION_ID by pcrf-core.	Call failure reported in overall performance output. Workaround: None	3	22.2.0
34645290	wrong policy decision (user with Quota)	Pcrf-core responds to CCA-I with usage Monitoring AVPs even when subscriber has provisioned quota and Blockly present but no grant action.	Unexpected quota grant occurs during UsageMon activation. Workaround: Disable the Monitoring Key with a blockly in policy project	3	22.2.2
34644483	PCF behavior on CHF selection when CHF uses pattern while Registration	Pcrf-core responds to CCA-I with usage Monitoring AVPs even when subscriber has provisioned quota and Blockly present but no grant action.	multiple CHF profiles restrict operators to operate with range provisioned. Workaround: CHF profile should be configured with Range if multiple profiles are being used.	3	22.1.0

Table 4-48 CNC Policy 22.3.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
34536372	PDS audit cleanup of stray session not working for Gx-Sy flow(4G)	PDS is unable to perform graceful termination of stray Sy session on audit cycle.	Concurrent messages can cause stale session to PDS context in 4G call flow. Workaround: None	3	22.1.2
34536333	bulk import for usage-monitoring configuration is failing	Bulk import for usage-monitoring configuration is failing.	Bulk Import for Usage Monitoring is reported as Failure even if the configurations are imported successfully. Workaround: User have to configure the Usage Monitoring Service manually.	3	
34477374	Usage Monitoring data from PDS databases is not deleted for stale profiles	PDS records related with UM data will not be deleted when the CCR-T is send.	PDS records related with UM data will not be deleted when the CCR-T is send. Workaround: None	3	22.2.0
34536257	Delete of SM Session using "Initiate Remote Session Cleanup" is not working	SM Session will not clean up if user tries to delete the remote sessions using "Initiate Remote Session Cleanup" from session viewer screen.	SM Session will not clean up if user tries to delete the remote sessions using "Initiate Remote Session Cleanup" from session viewer screen. Workaround: None	3	22.3.0

Table 4-48 (Cont.) CNC Policy 22.3.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
34454007	POLICY_OVERLOAD PCF/IGW rejecting SM Create request even if rate of execution is lesser than configured rate for RateLimiting Feature	PCF is rejecting SM Create request even if rate of execution is lesser than configured rate for RateLimiting Feature.	Customer Impact: Traffic may get rejected at Ingress GW even if the rate of execution is lesser than configured rate for RateLimiting Feature. Workaround: Set a rate limit value slightly greater than 2*(request rate sent per {route,method} combination) to avoid request failure due to inconsistency in request rate.	3	22.2.0
34555206	EGW is reporting "configJson is missing in the response from secondary instance of config client" ERROR	Egress GW is reporting "configJson is missing in the response from secondary instance of config client" Error log after every 5 seconds.	Egress GW is reporting "configJson is missing in the response from secondary instance of config client" Error log after every 5 seconds. Workaround: None	3	

Note:

The known bugs from CNC Policy Release 22.2.1, 22.2.2, and 22.2.3 are forward ported to Release 22.3.0.

4.3.7 NEF Known Bugs

NEF Release 22.3.2

There are no known bugs in this release.

NEF Release 22.3.1

There are no known bugs in this release.

NEF Release 22.3.0

There are no known bugs in this release.

4.3.8 NRF Known Bugs

Table 4-49 NRF 22.3.2 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
34839907	OCNRF Roaming MNC with 2 digits is treated as different with 3 digits when leading 0 value.	When there is a leading zero in the MNC value, the value is incorrectly used in the roaming scenario. For example: MCC-310 and MNC -14 are treated differently when compared with MCC-310 and MNC-014.	In case a leading zero is present in the MNC of PLMN attribute, it will impact the roaming scenario. This value is used to compare the requester PLMN in the incoming request and PLMN configured in OCNRF configuration. **Workaround:** If NFs are sending MNC with 0 appended, then OCNRF shall be configured with appended 0 in MNC.	3	22.3.1

Table 4-49 (Cont.) NRF 22.3.2 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 metric is not pegged for the artisan pod.	OcnrfReplicationStatusMonitoringInactive alert will be raised for the pod. **Workaround:** Update the alert expression to exclude nrfartisan service as specified below: sum by(pod) (irate(ocnrf_replication_status_check_total{container!~"nrfauditor|nrfartisan" }[5m])) == 0	3	22.3.2

NRF 22.3.1 Known Bugs

There are no new known bugs in this release. For existing known bugs, see NRF 22.3.0 Known Bugs.

Table 4-50 NRF 22.3.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
34426591	NRF not sending DNS update for already Registered AMFs after Enabling DNS feature	NRF not sending DNS update for already Registered AMFs after enabling DNS feature.	AMF registered after disabling and re-enabling DNS feature will not be updated in the DNS server. **Workaround:** In case of disabling the DNS NAPTR feature, do not register AMF, and update NAPTR specific AMF profile attributes until DNS NAPTR feature is enabled again. In case this behavior occurs, then in max after 30 mins OCNRF will detect the AMF register/ update changes. Status and Retrigger APIs can be used to register/ update the AMF details.	3	22.2.0

Table 4-50 (Cont.) NRF 22.3.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
34426552	NRF not removing DNS records for Registered AMFs after switching DNS feature flag to Disabled	As per requirement, NRF_AMF_DNS_FUNC_1040 : "operator when switches feature flag defined in NRF_AMF_DNS_CONF_1000 from ENABLED to DISABLED. All existing registered AMFs with AMFInfo --> N2InterfaceAmfInfo is removed from DNS Server with NAPTR records and A/AAAA records.	After disabling of the DNS feature, correspondin g AMF NAPTR records are still present in DNS server. **Workaround:** Remove such DNS NAPTR records manually.	3	22.2.0
34426530	NRF-DNS NAPTR Record not completely cleaned up from DNS after AMF-NF De-registration	NRF-DNS NAPTR Record not completely cleaned up from DNS after AMF-NF De-registration of multiple records.	Deregistration of one of the AMFs sharing *amfSetId*, *amfRegionId* and *amfName* are not removed from the DNS records properly. **Workaround:** Remove such DNS NAPTR records manually.	3	22.2.0

Table 4-50 (Cont.) NRF 22.3.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
34545093	NF_Register Request with nfProfileChangeInd not compliant	If NRF configured PLMN say MCCMNC 208-01 and in nfProfileregistration, 208-01 and 206-01. NRF saves nfProfile with 208-01 only but in the response NRF is not informing to consumer that 208-01 is only acceptedwhen nfProfileChangeInd is true. Need to check if The same is applicable also to perPlmnSnssaisList.	NF registration response with partial profile will not have updates for PLMN, if some of the PLMN values are dropped by NRF. **Workaround:** Use complete NFProfile instead only nfProfileChangeInd.	3	22.2.0
34549465	OCNRF headers processing shall be case insensitive	As per HTTP RFC 7230, HTTP header names should be case-insensitive. However the Header values are application defined. https://datatracker.ietf.org/doc/html/rfc7230#section-3.2.	Currently in NRF, headers having case-sensitive check. As part of this story,the check needs to be changed to work in case-insensitive manner. **Workaround:** Do not change the header case.	4	22.2.0

Table 4-50 (Cont.) NRF 22.3.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
34473746	NRF ocnrf_stale_nfSubscriptions_deleted_total metrics not getting pegged	Unable to see “ocnrf_stale_nfSubscriptions_deleted_total” metrics in prometheus.	Number of subscriptions deleted cannot be determined using this metrics. **Workaround:** None	4	22.1.0

4.3.9 NSSF Known Bugs

NSSF 22.3.2 Known Bugs

There are no new known bugs in this release. For existing known bugs, see NSSF 22.3.0 Known Bugs.

NSSF 22.3.1 Known Bugs

There are no new known bugs in this release. For existing known bugs, see NSSF 22.3.0 Known Bugs.

Table 4-51 NSSF 22.3.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
34427550	NSSF for NsAvailability PUT is responding with all supported SNSSAIs, instead of intersection	When ONSSAI is enabled, NSSF is responding with all S-NSSAIs instead of the intersected S-NSSAIs.	AMF can process only the S-NSSAIs supported by it. **Workaround**: None.	3	22.3.0

4.3.10 NWDAF Known Bugs

NWDAF 22.0.0 Known Bugs

There are no known bugs.

4.3.11 SCP Known Bugs

SCP 22.3.4 Known Bugs

There are no new known bugs in this release. For existing known bugs, see Table 4-52.

SCP 22.3.3 Known Bugs

There are no new known bugs in this release. For existing known bugs, see Table 4-52.

SCP 22.3.2 Known Bugs

There are no new known bugs in this release. For existing known bugs, see Table 4-52.

SCP 22.3.1 Known Bugs

There are no new known bugs in this release. For existing known bugs, see Table 4-52.

Table 4-52 SCP 22.3.0 Known Bugs

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

4.3.12 SEPP Known Bugs

SEPP Release 22.3.2

There are no known bugs in this release.

Table 4-53 SEPP Release 22.3.1 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
34498601	N32 IGW dropping traffic silently due to io.netty.util.IllegalReferenceCountException	All Inter PLMN traffic is silently dropped at N32 IGW when traffic is run for a long duration due to the following error: *io.netty.util.IllegalReferenceCountException* on netty threads. The issue is observed after sending traffic for 12 hours at 800 TPS. TPS: 800 TPS. Length of run: 12 hours. N32 EGW -> N32 IGW.	SEPP performance runs done for a long duration are impacted. **Workaround**: Some packets are dropped at IGW in a lab setup, but in customer deployments, the failed request will be retried on a different SEPP. Hence, the impact of this issue will be low. Also, it is an intermittent issue.	3	22.2.0
34533995	RemoteSEPP Delete REST API at config mgr returns success in case of underlying failures	The RemoteSEPP Delete REST API at config mgr service returns success in case of underlying failures.	RemoteSEPP remains in the database even after running the delete command. Ithappens randomly and not in all cases. **Workaround**: Delete REST API must be run after resolving the underlying issue.	4	22.3.0

Table 4-54 SEPP Release 22.3.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
34498601	N32 IGW dropping traffic silently due to io.netty.util.IllegalReferenceCountException	All Inter PLMN traffic is silently dropped at N32 IGW when traffic is run for a long duration due to the following error: *io.netty.util.IllegalReferenceCountException* on netty threads. The issue is observed after sending traffic for 12 hours at 800 TPS. TPS: 800 TPS. Length of run: 12 hours. N32 EGW -> N32 IGW.	SEPP performance runs done for a long duration are impacted. **Workaround**: Some packets are dropped at IGW in a lab setup, but in customer deployments, the failed request will be retried on a different SEPP. Hence, the impact of this issue will be low. Also, it is an intermittent issue.	3	22.2.0
34533995	RemoteSEPP Delete REST API at config mgr returns success in case of underlying failures	The RemoteSEPP Delete REST API at config mgr service returns success in case of underlying failures.	RemoteSEPP remains in the database even after running the delete command. Ithappens randomly and not in all cases. **Workaround**: Delete REST API must be run after resolving the underlying issue.	4	22.3.0
34534058	Handshake alert is not getting cleared in some error scenarios	The handshake failure alert raised is not getting cleared when the successful handshake is completed in some of the scenarios:1) when the handshake failure is due to incorrect FQDN2) When the handshake failure is due to incorrect plmn.	Alert remains visible in the Prometheus database. **Workaround**: The alert disappears on restarting the service.	4	22.3.0

4.3.13 UDR Known Bugs

UDR 22.3.4 Known Bugs

There are no new known bugs in this release. For existing known bugs, see Table 4-55

Table 4-55 UDR 22.3.3 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
34384541	LCI Header format for IGW contains load-metric value with decimal places > 3	The Load-Metric field should have maximum of three decimal digits.	This has no significant effect. **Workaround**: NA	3	22.2.0
34374953	ProvGw XML structure: End Tag mismatch in between 4G-UDR and 5G-UDR	Format of all the SOAP responses is not as per 4G UDR output because there is a mismatch in the End tag between the 4G UDR and 5G UDR.	The operation is successful but format of response needs to be changed as per 4G UDR output. **Workaround**: NA	3	22.2.0

UDR 22.3.2 Known Bugs

There are no new known bugs in this release. For existing known bugs, see Table 4-56.

UDR 22.3.1 Known Bugs

There are no new known bugs in this release. For existing known bugs, see Table 4-56.

Table 4-56 UDR 22.3.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
34502997	DELETE VSA for Single - Network Slice Selection Assistance Information(S-NSSSAI) is not deleting the subscriber	Subscriber is not deleted. If the VSA is configured at S-NSSA, the delete operation is partial.	No direct impact. VSA at SNSSAI is not being used for deployments. **Workaround**: NA	3	22.2.0

Table 4-56 (Cont.) UDR 22.3.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
34384541	LCI Header format for IGW contains load-metric value with decimal places > 3	The load metric value have decimal numbers that are more than 3 decimal places.	This has no significant effect. **Workaround**: NA	3	22.2.0
34374953	ProvGw XML structure: End Tag mismatch in between 4G-UDR and 5G-UDR	There is a end tag mismatch between 4G and 5G UDR because the response is not as per 4G UDR output.	The operation is successful but format of response needs to be changed as per 4G UDR output. **Workaround**: NA	3	22.2.0
34559281	nrf-client-nfmanagement pre upgrade fails during 22.2.1 to 22.3.0 upgrade	When upgrading from 22.2.x to 22.3.0 the nrf-client-nfmanagement pre upgrade fails due to issue in the charts.	Customer impact is considered to be low. **Workaround**: Manual update of charts are required.	3	22.3.0