Oracle® Communications

Cloud Native Core Release Notes

Release 2.22.2
F57774-25
March 2023

Oracle Communications Cloud Native Core Release Notes, Release 2.22.2

F57774-25

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 2.22.2 - F57774-25, March 2023

The following sections are updated for SCP 22.2.4:

- Media Pack: Updated the media pack details for SCP release 22.2.4.
- Compliance Matrix: Updated the compliance matrix information for SCP release 22.2.4.
- Common Microservices Load Lineup: Updated the common services load lineup details for SCP release 22.2.4.
- Security Certification Declaration : Added security declaration for SCP release 22.2.4.
- SCP Resolved Bugs: Added resolved bugs list for SCP release 22.2.4.
- SCP Known Bugs: Added known bugs list for SCP release 22.2.4.

Release 2.22.2 - F57774-24, February 2023

The following sections are updated for CNC Policy 22.2.6:

- 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 : Updated the security certification declaration details.
- CNC Policy Resolved Bugs: Added resolved bugs list for CNC Policy.
- CNC Policy Known Bugs: Added known bugs list for Policy.

Release 2.22.2 - F57774-23, January 2023

The following sections are updated for NEF 22.2.3:

- Media Pack: Updated media pack details for NEF release 22.2.3.
- Compliance Matrix: Updated the compliance matrix information for NEF release 22.2.3.
- Common Microservices Load Lineup: Updated the common services load lineup details for NEF release 22.2.3.
- Security Certification Declaration : Added security certification declaration for NEF release 22.2.3.
- NEF Resolved Bugs: Added resolved bugs list for NEF release 22.2.3.

The following sections are updated for CNE 22.2.3:

- Media Pack: Updated media pack details for CNE release 22.2.3.
- Compliance Matrix: Updated the compliance matrix information for CNE release 22.2.3.
- CNE Resolved Bugs: Added resolved bugs list for CNE release 22.2.3.

Release 2.22.2 - F57774-22, January 2023

The following sections are updated for DBTier 22.2.5:

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

Release 2.22.2 - F57774-21, January 2023

Updated the following sections with the details of CNC Policy 22.2.5

- 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 : Updated the security certification declaration details.
- CNC Policy Resolved Bugs: Added resolved bugs list for CNC Policy.
- CNC Policy Known Bugs: Added known bugs list for Policy.

Release 2.22.2 - F57774-20, December 2022

Added a bug under NRF 22.2.2 release in the NRF Known Bugs section.

Release 2.22.2 - F57774-19, November 2022

The following sections are updated for DBTier 22.2.4:

- Media Pack: Updated media pack details for DBTier release 22.2.4.
- Compliance Matrix: Updated the compliance matrix information for DBTier release 22.2.4.
- DBTier Resolved Bugs: Added known bugs list for DBTier release 22.2.4.

Release 2.22.2 - F57774-18, November 2022

There are no documentation updates in this version.

Release 2.22.2 - F57774-17, November 2022

Updated the following sections with the details of SCP 22.2.3:

- 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.
- SCP Resolved Bugs: Added resolved bugs list for SCP release 22.2.3.
- SCP Known Bugs: Added known bugs list for SCP release 22.2.3.

Release 2.22.2 - F57774-16, October 2022

Updated the following sections with the details of BSF 22.2.4, CNE 22.2.2, CNC Console 22.2.2, cnDBTier 22.2.3, NSSF 22.2.2, NRF 22.2.3, CNC Policy 22.2.4, SEPP 22.2.2, UDR 22.2.2:

- 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.
- CNE Resolved Bugs: Added resolved bugs list for CNE.
- CNC Console Resolved Bugs: Added resolved bugs list for CNC Console.
- DBTier Resolved Bugs: Added resolved bugs list for cnDBTier.
- CNC Policy Resolved Bugs: Added resolved bugs list for CNC Policy.
- NSSF Resolved Bugs: Added resolved bugs list for NSSF.
- UDR Resolved Bugs: Added resolved bugs list for UDR.
- CNC Policy Known Bugs: Added known bugs list for Policy.

Release 2.22.2 - F57774-15, October 2022

NEF Release 22.2.2
The following sections are updated for NEF 22.2.2:

- Media Pack: Updated media pack details for NEF release 22.2.2.
- Compliance Matrix: Updated the compliance matrix information for NEF release 22.2.2.
- Common Microservices Load Lineup: Updated the common services load lineup details for NEF release 22.2.2.
- Security Certification Declaration : Added security certification declaration for NEF release 22.2.2.

Release 2.22.2 - F57774-14, September 2022

CNE Release 22.2.2
The following sections are updated for CNE 22.2.2:

- Media Pack: Updated media pack details for CNE release 22.2.2.
- Compliance Matrix: Updated the compliance matrix information for CNE release 22.2.2.
- CNE Resolved Bugs: Added resolved bugs list for CNE release 22.2.2.
- CNE Known Bugs: Updated the known bugs list for CNE release 22.2.2.

Release 2.22.2 - F57774-13, September 2022

NRF Release 22.2.2
The following sections are updated for NRF 22.2.2:

- Media Pack: Updated the media pack details for NRF release 22.2.2.
- Compliance Matrix: Updated the compliance matrix information for NRF release 22.2.2.
- Common Microservices Load Lineup: Updated the common services load lineup details for NRF release 22.2.2.

- Security Certification Declaration : Added security certification declaration for NRF release 22.2.2.
- NRF Resolved Bugs: Added resolved bugs list for NRF release 22.2.2.

Release 2.22.2 - F57774-12, August 2022

SCP Release 22.2.2
The following sections are updated for SCP 22.2.2:

- Media Pack: Updated the media pack details for SCP release 22.2.2.
- Compliance Matrix: Updated the compliance matrix information for SCP release 22.2.2.
- Common Microservices Load Lineup: Updated the common services load lineup details for SCP release 22.2.2.
- SCP Resolved Bugs: Added resolved bugs list for SCP release 22.2.2.
- SCP Known Bugs: Added known bugs list for SCP release 22.2.2.

Release 2.22.2 - F57774-11, August 2022

CNC Policy Release 22.2.3
The following sections are updated for CNC Policy 22.2.3:

- Media Pack: Updated the media pack details for Policy release 22.2.3.
- Compliance Matrix: Updated the compliance matrix information for Policy release 22.2.3.
- Common Microservices Load Lineup: Updated the common services load lineup details for Policy release 22.2.3.
- CNC Policy Resolved Bugs: Added resolved bugs list for Policy release 22.2.3.

BSF Release 22.2.3
The following sections are updated for BSF 22.2.3:

- Binding Support Function (BSF): Added feature details for BSF release 22.2.3.
- Media Pack: Updated media pack details for BSF release 22.2.3.
- Compliance Matrix: Updated the compliance matrix information for BSF release 22.2.3.
- Common Microservices Load Lineup: Updated common services load lineup details for BSF release 22.2.3.

Release 2.22.2 - F57774-10, July 2022

DBTier Release 22.2.2
The following sections are updated for DBTier 22.2.2:

- Media Pack: Updated media pack details for DBTier release 22.2.2.
- Compliance Matrix: Updated the compliance matrix information for DBTier release 22.2.2.
- DBTier Resolved Bugs: Added known bugs list for DBTier release 22.2.2.

Release 2.22.2 - F57774-09, July 2022

CNC Policy Release 22.2.2
The following sections are updated for CNC Policy 22.2.2:

- Media Pack: Updated the media pack details for Policy release 22.2.2.
- Compliance Matrix: Updated the compliance matrix information for Policy release 22.2.2.

- Common Microservices Load Lineup: Updated the common services load lineup details for Policy release 22.2.2.
- CNC Policy Resolved Bugs: Added resolved bugs list for Policy release 22.2.2.

Release 2.22.2 - F57774-08, July 2022

NEF Release 22.2.1
The following sections are updated for NEF 22.2.1:

- Media Pack: Updated media pack details for NEF Release 22.2.1.
- Compliance Matrix: Updated the compliance matrix information for NEF Release 22.2.1.
- Common Microservices Load Lineup: Added common services load lineup details for NEF Release 22.2.1

SEPP Release 22.2.1
The following sections are updated for SEPP 22.2.1:

- Security Edge Protection Proxy (SEPP): Added the feature details for SEPP Release 22.2.1.
- Media Pack: Updated media pack details for SEPP Release 22.2.1.
- Compliance Matrix: Updated the compliance matrix information for SEPP Release 22.2.1.
- Common Microservices Load Lineup: Added common services load lineup details for SEPP Release 22.2.1
- SEPP Resolved Bugs: Added resolved bugs list for SEPP release 22.2.1.

Release 2.22.2 - F57774-07, July 2022

CNE Release 22.2.1
The following sections are updated for CNE 22.2.1:

- Media Pack: Updated media pack details for CNE release 22.2.1.
- Compliance Matrix: Updated the compliance matrix information for CNE release 22.2.1.
- CNE Resolved Bugs: Added known bugs list for CNE release 22.2.1.

CNC Policy Release 22.2.1
The following sections are updated for CNC Policy 22.2.1:

- Media Pack: Updated the media pack details for Policy release 22.2.1.
- Compliance Matrix: Updated the compliance matrix information for Policy release 22.2.1.
- Common Microservices Load Lineup: Updated the common services load lineup details for Policy release 22.2.1.
- CNC Policy Resolved Bugs: Added resolved bugs list for Policy release 22.2.1.
- CNC Policy Known Bugs: Added known bugs list for Policy release 22.2.1.

BSF Release 22.2.1
The following sections are updated for BSF 22.2.1:

- Binding Support Function (BSF): Added feature details for BSF release 22.2.1.

- Media Pack: Updated media pack details for BSF release 22.2.1.
- Compliance Matrix: Updated the compliance matrix information for BSF release 22.2.1.
- Common Microservices Load Lineup: Updated common services load lineup details for BSF release 22.2.1.

Release 2.22.2 - F57774-06, July 2022

DBTier Release 22.2.1
The following sections are updated for DBTier 22.2.1:

- Media Pack: Updated media pack details for DBTier release 22.2.1.
- Compliance Matrix: Updated the compliance matrix information for DBTier release 22.2.1.
- DBTier Resolved Bugs: Added known bugs list for DBTier release 22.2.1.
- DBTier Known Bugs: Added known bugs list for DBTier release 22.2.1.

CNC Console Release 22.2.1
The following sections are updated for CNC Console 22.2.1:

- Media Pack: Updated media pack details for CNC Console release 22.2.1.
- Compliance Matrix: Updated the compliance matrix information for CNC Console release 22.2.1.
- Common Microservices Load Lineup: Added common services load lineup details for CNC Console release 22.2.1.
- CNC Console Resolved Bugs: Added resolved bugs list for CNC Console release 22.2.1.

NRF Release 22.2.1

- Media Pack: Updated the media pack details for NRF release 22.2.1.
- Compliance Matrix: Updated the compliance matrix information for NRF release 22.2.1.
- Common Microservices Load Lineup: Updated the common services load lineup details for NRF release 22.2.1.
- NRF Resolved Bugs: Added resolved bugs list for NRF release 22.2.1.

NSSF Release 22.2.1

- Media Pack: Updated the media pack details for NSSF release 22.2.1.
- Compliance Matrix: Updated the compliance matrix information for NSSF release 22.2.1.
- Common Microservices Load Lineup: Updated the common services load lineup details for NSSF release 22.2.1.

SCP Release 22.2.1

- Media Pack: Updated the media pack details for SCP release 22.2.1.
- Compliance Matrix: Updated the compliance matrix information for SCP release 22.2.1.
- Common Microservices Load Lineup: Updated the common services load lineup details for SCP release 22.2.1.
- SCP Resolved Bugs: Added resolved bugs list for SCP release 22.2.1.
- SCP Known Bugs: Added known bugs list for SCP release 22.2.1.

UDR Release 22.2.1

- Media Pack: Updated the media pack details for UDR release 22.2.1.

- Compliance Matrix: Updated the compliance matrix information for UDR release 22.2.1.
- Common Microservices Load Lineup: Updated the common services load lineup details for UDR release 22.2.1.
- UDR Resolved Bugs: Added resolved bugs list for UDR release 22.2.1.
- UDR Known Bugs: Added known bugs list for UDR release 22.2.1.

Release 2.22.2 - F57774-05, June 2022

The following sections are updated for CNE 22.2.0:

- Cloud Native Environment (CNE): Added feature details for CNE release 22.2.0.
- Media Pack: Updated media pack details for CNE release 22.2.0.
- Compliance Matrix: Updated the compliance matrix information for CNE release 22.2.0.
- CNE Resolved Bugs: Added known bugs list for CNE release 22.2.0.
- CNE Known Bugs: Added known bugs list for CNE release 22.2.0.

Release 2.22.2 - F57774-04, June 2022

The following sections are updated for DBTier 22.2.0:

- Continuous Delivery Control Server (CDCS): Updated feature details for CDCS release 22.2.0 to include cnDBTier 22.2.0 compatibility.
- DBTier Known Bugs: Added known bugs list for DBTier release 22.2.0.

Release 2.22.2 - F57774-03, June 2022

The following section is updated:

- Compliance Matrix: Updated the OSO version for all NFs.

Release 2.22.2 - F57774-02, May 2022

ATS Release 22.2.0
The following sections are updated for ATS 22.2.0:

- Automated Testing Suite (ATS) Framework: Added feature details for ATS release 22.2.0.
- Media Pack: Updated media pack details for all the NFs that support ATS 22.2.0.

BSF Release 22.2.0
The following sections are updated for BSF 22.2.0:

- Binding Support Function (BSF): Added feature details for BSF release 22.2.0.
- Media Pack: Updated media pack details for BSF release 22.2.0.
- Compliance Matrix: Updated the compliance matrix information for BSF release 22.2.0.
- Common Microservices Load Lineup: Updated common services load lineup details for BSF release 22.2.0.
- Security Certification Declaration : Added security certification declaration for BSF release 22.2.0.

CNC Policy Release 22.2.0
The following sections are updated for CNC Policy 22.2.0:

- Cloud Native Core Policy (CNC Policy): Added the feature details for Policy release 22.2.0.
- Media Pack: Updated the media pack details for Policy release 22.2.0.
- Compliance Matrix: Updated the compliance matrix information for Policy release 22.2.0.
- Common Microservices Load Lineup: Updated the common services load lineup details for Policy release 22.2.0.
- CNC Policy Resolved Bugs: Added resolved bugs list for Policy release 22.2.0.
- CNC Policy Known Bugs: Added known bugs list for Policy release 22.2.0.

CNC Console Release 22.2.0
The following sections are updated for CNC Console 22.2.0:

- Cloud Native Core Console (CNC Console): Added the feature details for CNC Console release 22.2.0.
- Media Pack: Updated media pack details for CNC Console release 22.2.0.
- Compliance Matrix: Updated the compliance matrix information for CNC Console release 22.2.0.
- Common Microservices Load Lineup: Added common services load lineup details for CNC Console release 22.2.0.
- CNC Console Resolved Bugs: Added resolved bugs list for CNC Console release 22.2.0.

Release 2.22.2 - F57774-01, May 2022

This is an initial release of this document for Release 2.22.2.

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.x.

2.1 Automated Testing Suite (ATS) Framework

Oracle Communications Cloud Native Core Automated Test Suite (ATS) framework 22.2.0 has been updated with the following enhancements:

- **Application Log Collection:** Application Log Collection can be implemented by using either ElasticSearch or Kubernetes Logs. In both these implementations, logs are collected per scenario for the failed scenarios. For more information, see *Oracle Communications Cloud Native Core Automated Testing Suite Guide.*
- **ATS Jenkins Job Queue**: This feature provides the support of queuing the second job if the current job is already running whether from the same pipelines or different pipelines. For more information, see *Oracle Communications Cloud Native Core Automated Testing Suite Guide.*
- **ATS System Name and Version Display on Jenkins GUI:** With this feature, ATS system name and version are displayed on Jenkins GUI. For more information, see *Oracle Communications Cloud Native Core Automated Testing Suite Guide.*
- **PCAP Log Collection:** PCAP Log Collection allows collecting the NF, SUT, or PCAP logs from the debug tool side car container. For more information, see *Oracle Communications Cloud Native Core Automated Testing Suite Guide.*

2.2 Binding Support Function (BSF)

Release 22.2.4

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

Release 22.2.3

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

Release 22.2.1

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

Release 22.2.0

Oracle Communications Cloud Native Core Binding Support Function (BSF) 22.2.0 has been updated with the following enhancements:

- **Overload Control - Diameter Interface**: BSF supports the load shedding and overload control mechanisms for Diameter interface that reduce latency in overload situations and maintain the overall health of the system. With this feature, BSF avoids entering into overload condition, detects overload conditions, and then takes necessary actions to recover from the overload state. For more information on this feature and its configurations, see the "Overload Control - Diameter Interface" section in *Oracle Communications Cloud Native Core Binding Support Function User Guide*.

- **Overload Control and Handling - SBI Interface**: BSF supports the rate limiting and overload control for SBI interface that prevent service performance from degrading in an uncontrolled manner under heavy load. As BSF management service starts approaching its saturation or planned limit, response times typically grow high and throughput may degrade substantially. Under such conditions, it is desirable to shed load based on operator configuration, rather than cause all sessions and signaling flows to experience unacceptable response times or failures or downtime. For more information on this feature and its configurations, see the "Overload Control - SBI Interface" section in *Oracle Communications Cloud Native Core Binding Support Function User Guide*.
- **Stale Session Handling with PCF Interaction**: BSF supports the stale session handling feature as part of which the Audit service detects stale sessions automatically at regular intervals. During the audit, if the audit service finds records with a binding age greater than the configured value, it marks such records as suspected stale and notifies the BSF management service. Depending on the feature configurations, BSF may query PCF to confirm if the records are stale. If PCF confirms the record as stale, then BSF removes it from its local database. For more information on this feature and its configurations, see the "Stale Session Handling" section in *Oracle Communications Cloud Native Core Binding Support Function User Guide*.
- **BSF Observability Enhancements**: BSF metrics are enhanced to be adapted to the cloud-native infrastructure. For more information on this feature, see the "Binding Support Function Metrics" section in *Oracle Communications Cloud Native Core Binding Support Function User Guide*.
- **Detection and Handling of Late Arrival Requests**: BSF supports the detection and handling of late arrival requests to detect the response time for the components received in the headers from the PCF. For more information on how to configure this feature using CNC Console, see the "Detection and Handling of Late Arrival Requests" section in *Oracle Communications Cloud Native Core Binding Support Function User Guide*.
- **CNCC Support for Multicluster Deployment**: With this feature, BSF deployed in multiple Kubernetes clusters can be accessed using CNC Console. In a multicluster deployment, the CNC Console can manage BSF and OCCNE common services deployed in the remote Kubernetes clusters. For more information on this feature, see *Oracle Communications Cloud Native Core Binding Support Function User Guide*.
- **CNCC Support for Multiple Instance Deployment**: With this feature, multiple instances of BSF deployed within a Kubernetes cluster can be accessed using CNC Console. In a Multiple instances deployment, the CNC Console can manage multiple BSF instances and OCCNE common services deployed within a Kubernetes cluster. For more information, see *Oracle Communications Cloud Native Core Binding Support Function Guide*.

2.3 Continuous Delivery Control Server (CDCS)

The CD Control Server (CDCS) is a Continuous Delivery (CD) solution for the Oracle CNC product line. CDCS acts as a centralized location from which to perform lifecycle operations for CNC 5G NFs, and OCCNE, at multiple sites within a customer's network. This is the initial release of the CD Control Server. For more information about the CD Control Server, see *Oracle Communications Cloud Native Core CD Control Server User Guide* and *Oracle Communications Cloud Native Core CD Control Server Installation Guide*.

CD Control Server is compatible with the following NF versions:

- cnDBTier 22.2.0
- SCP 22.2.0
- SEPP 22.2.0

2.4 Cloud Native Core Console (CNC Console)

Oracle Communications Cloud Native Core Console (CNC Console) 22.2.0 has been updated with the following enhancement:

Release 22.2.2

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

Release 22.2.1

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

Release 22.2.0

- **Integrated NSSF with CNC Console**: With this feature, Network Slice Selection Function (NSSF) can be integrated with the CNC Console. The integration allows the users to configure NSSF using the CNC Console. For more information, see *Oracle Communications Cloud Native Core Console User Guide*.
- **Support for Multicluster Deployment for NFs**: CNC Console supports NF deployment across Kubernetes clusters using Manager CNC Console IAM (M-CNCC IAM), Manager CNC Console Core (M-CNCC Core), and Agent CNC Console Core (A-CNCC Core). In a multicluster deployment, the CNC Console can manage NFs and OCCNE common services deployed in the remote Kubernetes clusters. The multicluster deployment for the following NFs are supported:
  - SCP 22.2.0
  - NRF 22.2.0
  - UDR 22.2.0
  - SEPP 22.2.0
  - NSSF 22.2.0
  - BSF 22.2.0
  - POLICY 22.2.0 (Supports from 22.1.0 onwards)

  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*.
- **Support for Multiple Instances of NFs within a cluster**: CNC Console supports multiple instances of NFs within a Kubernetes cluster using Manager CNC Console IAM (M-CNCC IAM), Manager CNC Console Core (M-CNCC Core), and Agent CNC Console Core (A-CNCC Core). The multiple instances of the following NFs are supported:
  - SCP 22.2.0

  - NRF 22.2.0
  - UDR 22.2.0
  - BSF 22.2.0
  - POLICY 22.2.0 (Supports from 22.1.0 onwards)

  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*.

- **Support for Ephemeral Storage**: CNC Console supports the configuration of ephemeral containers for the temporary storage of data of instances. The Pods use ephemeral local storage for scratch space, caching, and logs. For more information about ephemeral storage resource requirements, 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 22.2.0
  - NRF 22.2.0
  - UDR 22.2.0
  - SEPP 22.2.0
  - NSSF 22.2.0
  - BSF 22.2.0
  - POLICY 22.2.0

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)

Release 22.2.5

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

Release 22.2.4

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

Release 22.2.3

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

Release 22.2.2

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

Release 22.2.1

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

Release 22.2.0

Oracle Communications Cloud Native Core DBTier (cnDBTier) 22.2.0 has been updated with the following enhancements:

- **Support for DBTier Dual Stack Support**: DBTier is validated on an IPv6 mode in dual stack Kubernetes cluster. For more information about the parameter to configure IPv6, see *Oracle Communications Cloud Native Core DBTier Installation and Upgrade Guide.*
- **Support for DBTier roll back**: Rollback is supported from DBTier version 22.2.x to release 22.1.x and release 1.10.x. For more information about the rollback, see *Oracle Communications Cloud Native Core DBTier Installation and Upgrade Guide.*
- **Support for TLS for Georeplication**: DBTier TLS procedure is extended to provide manual steps to DBTier customer(s) to enable TLS support for the Georeplication channels between three and four mate sites. For more information about the TPS procedure, see *Oracle Communications Cloud Native Core DBTier User Guide.*
- **Support for DBTier Multus CNI:** DBTier supports Multus Container Network Interface (CNI). For more information about the Multus CNI, see *Oracle Communications Cloud Native Core DBTier Installation and Upgrade Guide.*

2.6 Cloud Native Core Policy (CNC Policy)

Release 22.2.6

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

Release 22.2.5

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

Release 22.2.4

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

Release 22.2.3

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

Release 22.2.2

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

Release 22.2.1

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

Release 22.2.0

Oracle Communications Cloud Native Core Policy 22.2.0 has been updated with the following enhancements:

- **Overload Control and Handling - SBI Interface**: CNC Policy supports the rate limiting and overload control for SBI interface that prevent service performance from degrading in an uncontrolled manner under heavy load. As CNC Policy microservices start approaching their planned limit, response times typically grow high and throughput may degrade substantially. Under such conditions, it is desirable to shed load based on operator configuration, rather than cause all sessions and signaling flows to experience unacceptable response times or failures or downtime. For more information on this feature and its configurations, see the "Overload Control - SBI Interface" section in *Oracle Communications Cloud Native Core Policy User Guide*.

- **Support for Usage Monitoring in PCRF Core**: CNC Policy supports Usage Monitoring service, an internal service that interacts with Policy PRE service to get usage monitoring related Policy decisions. Using this internal service, CNC Policy can apply usage monitoring control at session level. The usage can be defined as either volume or time of user plane traffic. Currently, Usage Monitoring service is supported for PCRF only. For more information, see "Usage Monitoring Service" in *Oracle Communications Cloud Native Core Policy User Guide*.
- **PCF Registration Status on NRF from CNC Console** - CNC Policy GUI is enhanced to include a new page - **NRF Status** under the **Status and Query** page in the CNC Console. Using this page, users can get a consolidated status of the PCF registered with NRF and also displays the autonomously discovered NFs details like CHF and BSF . This new page displays the health status of primary and secondary NRFs, or alternate NRF as well. For more information on this feature and its configurations, see *Oracle Communications Cloud Native Core Policy User Guide*.
- **NetLoc Support:** CNC Policy supports NetLoc which helps in fetching User Equipment (UE) time zone information and User location information from the access network. Such information is called Network Provided Location Information (NPLI). For more information on this feature and its configurations, see the "NetLoc Support" section in *Oracle Communications Cloud Native Core Policy User Guide*.
- **Subscription to Notification Support for Signaling Path Status:** CNC Policy supports notification, subscription to notification, and cancellation of subscription to notification of 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*.
- **SBI Timer Handling Enhancements:** CNC Policy is enhanced to configure timer per message type on Nudr and Nnrf SBI interfaces. For more information on this feature and its configurations, see the "SBI Timer Handling Enhancements" section in *Oracle Communications Cloud Native Core Policy User Guide*.
- **UE Policy Enhancements:** CNC Policy is enhanced to support UE Route Selection Policy (URSP) for transferring fragmented UE Policy and handling N1N2Message transfer Failure. For more information on this feature and its configurations, see the "UE Policy Enhancements" section in *Oracle Communications Cloud Native Core Policy User Guide*.
- **Support for Detection and Handling of Late Arrival Requests:** CNC Policy is enhanced to support the detection and handling of late arrival functionality in BSF. For more information on this feature and its configurations, see the "PCF Support for Detection and Handling of Late Arrival Requests in BSF" section in *Oracle Communications Cloud Native Core Policy User Guide*.
- **Support for Subscriber Notification - HTTP**: CNC Policy supports Notifier service that allows CNC Policy to send notifications (HTTP messages) to the subscribers about their current data usage. This service is independent of deployment mode and can be enabled in all the supported deployment modes. For more information on this feature, see the "Notifier service" section in *Oracle Communications Cloud Native Core Policy User Guide*.

- **Operator Specific Data support for 4G Subscriber over N36 Interface**: With this feature, CNC Policy supports retrieving operator specific data from PCRF core on nUDR interface on receiving Gx query. For more information, see *Oracle Communications Cloud Native Core Policy User Guide*.
- **Session Retry with NF Sets**: CNC Policy supports enhanced session retry and alternate routing mechanisms based on NRF Discovery and rediscovery for initial messages and DNS SRV based for subsequent messages in indirect communication model for AM and UE services. For more information on this feature, see the "Session Retry" section in *Oracle Communications Cloud Native Core Policy User Guide*.
- **Support for Stale Binding Detection in BSF**: To support BSF to query PCF for suspected stale binding records, the Binding service has been made mandatory in the PCF mode of deployment. In BSF, whenever a binding record is detected as stale on the expiry of its binding age, BSF may send a query to PCF to confirm its status. To support this query to PCF, PCF is first required to send the Vendor-Specific-Attribute containing PCF Notification URL in the Binding Register request. When PCF sends the Vendor-Specific-Attribute in the register request, it is also required to provide the vendorID. For more information on this feature, see *Oracle Communications Cloud Native Core Converged Policy User Guide.*
- **CNCC Support for Multicluster Deployment:** With this feature, CNC Policy deployed in multiple Kubernetes clusters can be accessed using CNC Console. In a multicluster deployment, the CNC Console can manage CNC Policy and OCCNE common services deployed in the remote Kubernetes clusters. For more information on this feature, see *Oracle Communications Cloud Native Core Converged Policy User Guide.*
- **CNCC Support for Multiple Instance Deployment:** With this feature, multiple instances of CNC Policy deployed within a Kubernetes cluster can be accessed using CNC Console. In a Multiple instances deployment, the CNC Console can manage multiple CNC Policy instances and OCCNE common services deployed within a Kubernetes cluster. For more information, see *Oracle Communications Cloud Native Core Converged Policy User Guide.*

2.7 Cloud Native Environment (CNE)

Release 22.2.3

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

Release 22.2.2

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

Release 22.2.1

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

Release 22.2.0

Oracle Communications Cloud Native Environment (OCCNE) 22.2.0 has been updated with the following enhancements:

- **Encrypted Kubernetes Secrets with key renewal:** OCCNE supports automatic encryption of all Secrets stored in the Kubernetes cluster. The key used to encrypt the secrets can be rotated as necessary. For more information about the feature, see *Oracle Communications Cloud Native Environment User Guide*.

- **Supports the Upgraded versions of Cloud Native Platform Services**: OCCNE supports the following upgraded versions of cloud native platform services:
  - Helm - 3.8.0
  - Kubernetes - 1.22.5
  - containerd - 1.5.8
  - Calico - 3.20.3
  - MetalLB - 0.12.1
  - Rook (BM installations only) - 1.8.4
  - Prometheus - 2.32.1
  - Grafana - 7.5.11
  - Elasticsearch - 7.9.3
  - Kibana - 7.9.3
  - Jaeger - 1.28.0
  - Istio - 1.12.1
  - cert-manager - 1.6.1

2.8 Network Exposure Function (NEF)

Release 22.2.2

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

Release 22.2.1

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

Release 22.2.0

Oracle Communications Cloud Native Core Network Exposure Function (NEF) 22.2.0 has been updated with the following enhancements:

GMLC Based Location Monitoring: OCNEF is enhanced to support the Gateway Mobile Location Center (GMLC) Based Location Monitoring feature. This feature enables OCNEF to report the highly accurate location details of subscribers with their geographic information through GMLC. For more information about the feature, see *Oracle Communications Cloud Native Core Network Exposure Function User Guide*.

Support for Model-D Indirect Communication: OCNEF supports the Model-D of the indirect communication method. This feature enables OCNEF to configure the necessary discovery and selection parameters required to find a suitable producer NF for handling a service request through SCP. For more information about the feature, see *Oracle Communications Cloud Native Core Network Exposure Function User Guide*.

OCNEF Exposure Gateway Event Management: The OCNEF architecture is enhanced to support the Event Manager service that enables OCNEF to notify Application Functions (AFs) or other internal services about the events occurring at the Exposure Gateway. For more information about the feature, see *Oracle Communications Cloud Native Core Network Exposure Function User Guide*.

Support for PodDisruptionBudget: OCNEF supports the PodDisruptionBudget (PDB) Kubernetes resource to provide high availability of scalable application services. For more information about the PDB specifications, see *Oracle Communications Cloud Native Core Network Exposure Function Installation Guide*.

2.9 Network Repository Function (NRF)

OCNRF Release 22.2.3

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

OCNRF Release 22.2.2

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

OCNRF Release 22.2.1

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

OCNRF Release 22.2.0

Oracle Communications Cloud Native Core Network Repository Functions (NRF) 22.2.0 has been updated with the following enhancements:

- **Support for EmptyList in Discovery Response**: When the feature is enabled, if all the matching profiles for a discovery request are in "SUSPENDED" state, OCNRF allows to change the profile state to "REGISTERED" by configuring a shorter validity period. For more information about the feature, see *Oracle Communications Cloud Native Core Network Repository Function User Guide*.
- **Support for Overload Control based on Percentage Discards**: OCNRF supports overload control to protect the nfregister, nfdiscovery, and nfaccesstoken services from overload situations and maintain the overall health of the services. 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. For more information about the feature, see *Oracle Communications Cloud Native Core Network Repository Function User Guide*.
- **Support for PodDisruptionBudget**: PodDisruptionBudget (PDB) is a Kubernetes resource that allows you to achieve high availability of scalable application services when the cluster administrators perform voluntary disruptions to manage the cluster nodes. For more information about the feature and the list of services supporting PDB, see *Oracle Communications Cloud Native Core Network Repository Function Installation and Upgrade Guide.*
- **Support for nfServiceList Map Attribute in NF Profile**: OCNRF now supports nfServiceList attribute (as per 3GPP Specification 3GPP TS 29.510 v16.7.0) in the NFProfile data type to include the map of NF service Instances, where the "serviceInstanceId" attribute of the NFService object is used as the key of the map. This map attribute includes the services produced by the NF that can be discovered by other NFs, if any.
- **Support for Tai attribute for UPF Profiles**: OCNRF supports User Plane Function (UPF) discovery based on discovery query parameter such as Tracking Area Identity (tai) and preferred Tracking Area Identity (preferred-tai). When OCNRF receives a discovery request with UpfInfo attribute, it processes the request based on the UPF profiles that can serve the TAI. For more information, see 3GPP Specification 3GPP TS 29.510 v16.7.0.

- **Support for 3gpp-Sbi-Correlation-Info header**: OCNRF supports 3gpp-Sbi-Correlation-Info header to enable network analytic tools or probes to easily identify the messages exchanged for a given User Equipment (UE). The Network Function (NF) service consumer or NF service producer can include any one of the UE identifiers (such as imsi, msisdn, extiid) in its 3gpp-Sbi-Correlation-Info header. The identifier helps to identify the UE related to the HTTP request or response. For more information about the `add3gppSbiCorrelationInfoHeader` parameter, see *Oracle Communications Cloud Native Core Network Repository Function User Guide.*
- **Support for DNS NAPTR Update**: OCNRF supports updating the Name Authority Pointer (NAPTR) record in Domain Name System (DNS) during Access and Mobility Functions (AMF) registration, update, and deregistration. For more information about the feature, see *Oracle Communications Cloud Native Core Network Repository Function User Guide.*
- **Support for Multicluster Deployment:** With this feature, OCNRF deployed in multiple Kubernetes clusters can be accessed using CNC Console. In a multicluster deployment, the CNC Console can manage OCNRF and OCCNE common services deployed in the remote Kubernetes clusters. For more information on this feature, see For more information about single and multiple cluster deployments, see *Oracle Communications Cloud Native Core Network Repository Function User Guide.*
- **Support for Multiple Instance Deployment:** With this feature, multiple instances of OCNRF deployed within a Kubernetes cluster can be accessed using CNC Console. In a Multiple instances deployment, the CNC Console can manage multiple OCNRF instances and OCCNE common services deployed within a Kubernetes cluster. For more information, see *Oracle Communications Cloud Native Core Network Repository Function User Guide.*

2.10 Network Slice Selection Function (NSSF)

Release 22.2.2

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

Release 22.2.1

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

Release 22.2.0

Oracle Communications Network Slice Selection Function (NSSF) 22.2.0 has been updated with the following enhancements:

- **Support for CNC Console**: Starting with this release, OCNSSF support CNC Console to configure the managed objects. For more information, see "Configuring OCNSSF Using CNC Console" in *Oracle Communications Cloud Native Core Network Slice Selection Function User Guide*.
- **Support for three-sites Georedundancy**: OCNSSF supports up to three-sites Georedundancy to ensure service continuity when one of the OCNSSF sites is down. For more information, see "Georedundancy" in *Oracle Communications Cloud Native Core Network Slice Selection Function User Guide*.
- **Support for Multicluster Deployment:** With this feature, OCNSSF deployed in multiple Kubernetes clusters can be accessed using CNC Console. In a

multicluster deployment, the CNC Console can manage OCNSSF and OCCNE common services deployed in the remote Kubernetes clusters. For more information on this feature, see *Oracle Communications Cloud Native Core Network Slice Selection Function User Guide.*

- **Support for Multiple Instance Deployment:** With this feature, multiple instances of OCNSSF deployed within a Kubernetes cluster can be accessed using CNC Console. In a Multiple instances deployment, the CNC Console can manage multiple OCNSSF instances and OCCNE common services deployed within a Kubernetes cluster. For more information on this feature, see *Oracle Communications Cloud Native Core Network Slice Selection Function User Guide.*
- **Support for PodDisruptionBudget**: PodDisruptionBudget (PDB) is a Kubernetes resource that allows you to achieve high availability of scalable application services when the cluster administrators perform voluntary disruptions to manage the cluster nodes. For more information about the feature and the list of services supporting PDB, see *Oracle Communications Cloud Native Core Network Slice Selection Function Installation and Upgrade Guide.*

2.11 Service Communication Proxy (SCP)

Release 22.2.4

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

Release 22.2.3

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

Release 22.2.2

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

Release 22.2.1

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

Release 22.2.0

Oracle Communications Cloud Native Core Service Communication Proxy (SCP) 22.2.0 has been updated with the following enhancements:

- **Support for SCP Deployment using Continuous Delivery Control Server (CDCS)**: In addition to SCP's Command Line Interface (CLI) deployment method, SCP can be deployed using Continuous Delivery Control Server (CDCS), which is a centralized server that automates SCP deployment processes such as downloading the SCP package, installation, upgrade, and rollback. For more information about CDCS, see *Oracle Communications Cloud Native Core CD Control Server User Guide*. For information about SCP deployment using CDCS, see *Oracle Communications Cloud Native Core Service Communication Proxy Installation and Upgrade Guide.*
- **Support for Alternate Routing Using Static Configuration**: This feature enables operators to configure a pair or combination of primary NFs and their alternate NFs to define alternate producer NFs, which can be used in alternate NF selection when routing attempt to the primary NF fails. For more information, see *Oracle Communications Cloud Native Core Service Communication Proxy User Guide.*

- **Aspen Service Mesh (ASM) Data Plane Configuration using Helm**: This feature automates the process of ASM data plane configuration through Helm. For more information, see *Oracle Communications Cloud Native Core Service Communication Proxy Installation and Upgrade Guide.*
- **5G SBI Message Mediation Support**: The existing Mediation functionality is enhanced to enable 5G HTTP2 message manipulation techniques to allow modification of Hypertext Transfer Protocol (HTTP) headers and JSON body parameters. SCP manipulates the incoming HTTP message requests based on the configured rules and responds with the manipulated message to NFs. For more information, see *Oracle Communications Cloud Native Core Service Communication Proxy User Guide.*
- **Global Egress Rate Limiting**: This feature synchronizes and aggregates the egress rate data for multiple producer NFs among multiple SCP instances (up to three SCP instances). Based on the aggregated rate data, each SCP controls its traffic to ensure that the global configured egress rate is achieved. For more information, see *Oracle Communications Cloud Native Core Service Communication Proxy User Guide.*
- **Support for Multicluster Deployment**: With this feature, SCP deployed in multiple Kubernetes clusters can be accessed using CNC Console. In a multicluster deployment, the CNC Console can manage SCP and OCCNE common services deployed in the remote Kubernetes clusters. For more information on this feature, see *Oracle Communications Cloud Native Core Service Communication Proxy User Guide.*
- **Support for Multiple Instances Deployment**: With the support of multiple instance deployment, a single instance of the CNC Console can configure two instances of SCP deployments if both CNC Console and SCP instances are deployed in the same Kubernetes cluster with different namespaces. For more information, see *Oracle Communications Cloud Native Core Service Communication Proxy User Guide*.

2.12 Security Edge Protection Proxy (SEPP)

OCSEPP Release 22.2.2

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

OCSEPP Release 22.2.1

Oracle Communications Cloud Native Core Security Edge Protection Proxy (SEPP) 22.2.1 has been updated with the following enhancements:

- **Support for Upgrade and Rollback**: Oracle Communications Cloud Native Core Security Edge Protection Proxy (SEPP) supports upgrade and rollback from release 22.2.0 to 22.2.1. For more information about the upgrade procedure, see *Oracle Communications Cloud Native Core Security Edge Protection Proxy Installation and Upgrade Guide.*

OCSEPP Release 22.2.0

Oracle Communications Cloud Native Core Security Edge Protection Proxy (SEPP) 22.2.0 has been updated with the following enhancements:

- **Global Rate limiting on ingress gateway of OCSEPP**: Global rate limiting, feature provided by Ingress Gateway (plmn-ingress-gateway and n32-ingress-

gateway), secures the network when aggregated Ingress traffic from any registered NF instance 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. With this feature, OCSEPP allows the user to configure the acceptable traffic rate from a consumer NF instance as well as configure the maximum number of incoming messages in the given duration.
For more information about the feature, see *Oracle Communications Cloud Native Core Security Edge Protection Proxy User Guide* and *Oracle Communications Cloud Native Core Security Edge Protection Proxy Installation Guide*.

- **Support of SEPP deployment through CDCS**: Along with the existing Command Line Interface deployment method, OCSEPP can be deployed using Continuous Delivery Control Server (CDCS), which is a centralized server that automates OCSEPP deployment processes. CD Automation feature solves the manual procedures and provides a continuous download, staging, and deployment model. For more information about CDCS, see *Oracle Communications Cloud Native Core CD Control Server User Guide* and *Oracle Communications Cloud Native Core Security Edge Protection Proxy Installation Guide*.
- **Support for Multicluster Deployment**: Multicluster is a method of deploying an application on or across multiple Kubernetes clusters for improving availability, isolation, and scalability. In a multicluster deployment, the CNC Console can manage OCSEPP deployed in the local or remote Kubernetes clusters.
  For more information about the feature, see *Oracle Communications Cloud Native Core Security Edge Protection Proxy User Guide*.
- **Support for PodDisruptionBudget**: PodDisruptionBudget (PDB) is a Kubernetes resource that allows you to achieve high availability of scalable application services when the cluster administrators perform voluntary disruptions to manage the cluster nodes. OCSEPP supports pod disruption budget to enable the availability of minimum replicas for microservices. For more information about the feature, see *Oracle Communications Cloud Native Core Security Edge Protection Proxy Installation Guide*.
- **Integrated Debug tool**: The Debug Tool provides third-party troubleshooting tools for debugging the runtime issues for the lab and production environment. Following are the available tools:
  - tcpdump
  - ip
  - netstat
  - curl
  - ping
  - dig

  For more information about the tools, see *Oracle Communications Cloud Native Core Security Edge Protection Proxy Troubleshooting Guide*.
- **Support for Server Header**: OCSEPP supports server header in the error responses generated for OCSEPP services. Using the server header, the user can find out if the error is generated either by the OCSEPP or some other NF. For more information about the feature, see *Oracle Communications Cloud Native Core Security Edge Protection Proxy User Guide*.
- **Support for Ephemeral Storage**: OCSEPP supports the configuration of ephemeral containers for the temporary storage of data of your instances. The Pods use ephemeral local storage for scratch space, caching, and logs. For more information about ephemeral

storage resource requirements, see *Oracle Communications Cloud Native Core Security Edge Protection Proxy Installation Guide*.

2.13 Unified Data Repository (UDR)

Release 22.2.2

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

Release 22.2.1

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

Release 22.2.0

Oracle Communications Cloud Native Core Unified Data Repository (UDR) 22.2.0 has been updated with the following enhancements:

- **Support for LCI and OCI Header:** With this feature, UDR supports Load Control Information (LCI) and Overload Control Information (OCI) Headers in Ingress Gateway and Egress Gateway. These headers convey the operating status of the producer resources to the consumer NFs. For more information, see *Oracle Communications Cloud Native Core Unified Data Repository User Guide*.
- **Segregation of Ingress Gateway for provisioning and signaling traffic:** With this enhancement, UDR supports Ingress Gateway instances for signaling and provisioning. For more information, see *Oracle Communications Cloud Native Core Unified Data Repository User Guide*.
- **Support for Multicluster Deployment**: With this feature, UDR and SLF deployed in multiple Kubernetes clusters can be accessed using CNC Console. In a multicluster deployment, the CNC Console can manage UDR and SLF and OCCNE common services deployed in the remote Kubernetes clusters. For more information on this feature, see *Oracle Communications Cloud Native Core Unified Data Repository User Guide*.
- **Support for Multiple Instances Deployment**: With the support of multiple instance deployment, a single instance of the CNC Console can configure two instances of UDR and SLF deployments if both CNC Console and UDR and SLF instances are deployed in the same Kubernetes cluster with different namespaces. For more information, see *Oracle Communications Cloud Native Core Unified Data Repository User Guide*.
- **Support for Taints or Tolerations and Node selector**: With this enhancement, UDR or SLF charts support configuring Taints or Tolerations and Node Selector. For more information, see *Oracle Communications Cloud Native Core Unified Data Repository User Guide*.
- **PDB Enhancements**: With this enhancement, microservices such as app-info, perf-info, config-server, Nudr-config, and NRF-client support multiple pods (HA) and PDBs. For more information, see *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 2.22.2. To download the media package, see MOS.

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

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

Table 3-1 Media Pack Contents for Cloud Native Core 2.22.2

Description	NF Version	ATS Version	Upgrade Supported
Oracle Communications Cloud Native Core Binding Support Function (BSF)	22.2.4	22.2.2	BSF 22.2.4 supports fresh installation and upgrade from 1.11.x or 22.1.x to 22.2.4. For more information on installation or upgrading, see *Oracle Communications Cloud Native Core Binding Support Function Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core Binding Support Function (BSF)	22.2.3	22.2.3	BSF 22.2.3 supports fresh installation and upgrade support from 1.11.x and 22.1.x to 22.2.3. For more information on installation or upgrading, see *Oracle Communications Cloud Native Core Binding Support Function Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core Binding Support Function (BSF)	22.2.1	22.2.1	BSF 22.2.1 supports fresh installation and upgrade from 1.11.x and 22.1.x to 22.2.1. For more information on installation or upgrading, see *Oracle Communications Cloud Native Core Binding Support Function Installation and Upgrade Guide*.

Table 3-1 (Cont.) Media Pack Contents for Cloud Native Core 2.22.2

Description	NF Version	ATS Version	Upgrade Supported
Oracle Communications Cloud Native Core Binding Support Function (BSF)	22.2.0	22.2.0	BSF 22.2.0 supports fresh installation and upgrade from 1.11.x and 22.1.x to 22.2.0. For more information on installation or upgrading, see *Oracle Communications Cloud Native Core Binding Support Function Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core Console (CNCC)	22.2.2	NA	CNC Console 22.2.0 supports fresh installation and upgrade from 1.9.x, 22.1.x, 22.2.x to 22.2.2. For more information on installation, see *Oracle Communications Cloud Native Core Console Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core Console (CNCC)	22.2.1	NA	CNC Console 22.2.1 supports fresh installation and upgrade from 22.1.x, 22.2.0 to 22.2.1. For more information on installation, see *Oracle Communications Cloud Native Core Console Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core Console (CNCC)	22.2.0	NA	CNC Console 22.2.0 supports fresh installation and upgrade from 1.9.x, 22.1.x to 22.2.0. For more information on installation, see *Oracle Communications Cloud Native Core Console Installation and Upgrade Guide*.
Oracle Communications Cloud Native Environment (OCCNE)	22.2.3	NA	OCCNE 22.2.3 supports fresh installation and upgrade from 22.1.x and 22.2.x to 22.2.3. 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 (OCCNE)	22.2.2	NA	OCCNE 22.2.2 supports fresh installation and upgrade from 22.1.x and 22.2.x to 22.2.2. 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 2.22.2

Description	NF Version	ATS Version	Upgrade Supported
Oracle Communications Cloud Native Environment (OCCNE)	22.2.1	NA	OCCNE 22.2.1 supports fresh installation and upgrade from 22.1.x and 22.2.0 to 22.2.1. 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 (OCCNE)	22.2.0	NA	OCCNE 22.2.0 supports fresh installation and upgrade from 22.1.x to 22.2.0. 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*.
Oracle Communications Cloud Native Core CD Control Server	22.2.0	NA	CD Control Server 22.2.0 supports fresh installation only. For more information on installation, see *Oracle Communications Cloud Native Core CD Control Server Installation Guide*.
Oracle Communications Cloud Native Core DBTier	22.2.5	NA	DBTier 22.2.5 supports fresh installation and upgrade from 1.10.x, 22.1.x, and 22.2.x to 22.2.5. For more information on installation, see *Oracle Communications Cloud Native Core DBTier Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core DBTier	22.2.4	NA	DBTier 22.2.4 supports fresh installation and upgrade from 1.10.x, 22.1.x, and 22.2.x to 22.2.4. For more information on installation, see *Oracle Communications Cloud Native Core DBTier Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core DBTier	22.2.3	NA	DBTier 22.2.3 supports fresh installation and upgrade from 1.10.x, 22.1.x, and 22.2.x to 22.2.3. 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 2.22.2

Description	NF Version	ATS Version	Upgrade Supported
Oracle Communications Cloud Native Core DBTier	22.2.2	NA	DBTier 22.2.2 supports fresh installation and upgrade from 1.10.x, 22.1.x, and 22.2.x to 22.2.2. For more information on installation, see *Oracle Communications Cloud Native Core DBTier Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core DBTier	22.2.1	NA	DBTier 22.2.1 supports fresh installation and upgrade from 1.10.x, 22.1.x, and 22.2.0 to 22.2.1. For more information on installation, see *Oracle Communications Cloud Native Core DBTier Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core DBTier	22.2.0	NA	DBTier 22.2.0 supports fresh installation and upgrade from 1.10.x and 22.1.x to 22.2.0. For more information on installation, see *Oracle Communications Cloud Native Core DBTier Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core Network Exposure Function (NEF)	22.2.3	NA	OCNEF 22.2.3 supports fresh installation only. For more information on installation, see *Oracle Communications Cloud Native Core Network Exposure Function Installation Guide*.
Oracle Communications Cloud Native Core Network Exposure Function (NEF)	22.2.2	22.2.2	OCNEF 22.2.2 supports fresh installation only. For more information on installation, see *Oracle Communications Cloud Native Core Network Exposure Function Installation Guide*.
Oracle Communications Cloud Native Core Network Exposure Function (NEF)	22.2.1	22.2.1	OCNEF 22.2.1 supports fresh installation only. For more information on installation, see *Oracle Communications Cloud Native Core Network Exposure Function Installation Guide*.
Oracle Communications Cloud Native Core Network Exposure Function (NEF)	22.2.0	22.2.0	OCNEF 22.2.0 supports fresh installation only. For more information on installation, see *Oracle Communications Cloud Native Core Network Exposure Function Installation Guide*.

Table 3-1 (Cont.) Media Pack Contents for Cloud Native Core 2.22.2

Description	NF Version	ATS Version	Upgrade Supported
Oracle Communications Cloud Native Core Network Repository Function (NRF)	22.2.3	22.2.3	OCNRF 22.2.3 supports fresh installation and upgrade from 22.1.x, 22.2.x to 22.2.3. 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)	22.2.2	22.2.2	OCNRF 22.2.2 supports fresh installation and upgrade from 22.1.x, 22.2.x to 22.2.2. 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)	22.2.1	22.2.1	OCNRF 22.2.1 supports fresh installation and upgrade from 22.1.x, 22.2.0 to 22.2.1. 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)	22.2.0	22.2.0	OCNRF 22.2.0 supports fresh installation and upgrade from 22.1.x to 22.2.0. 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)	22.2.2	22.2.2	OCNSSF 22.2.2 supports fresh installation only. 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)	22.2.1	22.2.1	OCNSSF 22.2.1 supports fresh installation only. 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)	22.2.0	22.2.0	OCNSSF 22.2.0 supports fresh installation only. 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 2.22.2

Description	NF Version	ATS Version	Upgrade Supported
Oracle Communications Cloud Native Core Policy (CNC Policy)	22.2.6	22.2.4	CNC Policy 22.2.6 supports fresh installation and upgrade from 1.15.x, 22.1.x, and 22.2.x to 22.2.6. For more information on installation or upgrading, see *Oracle Communications Cloud Native Core Converged Policy Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core Policy (CNC Policy)	22.2.5	22.2.2	CNC Policy 22.2.5 supports fresh installation and upgrade from 1.15.x, 22.1.x, and 22.2.x to 22.2.5. For more information on installation or upgrading, see *Oracle Communications Cloud Native Core Converged Policy Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core Policy (CNC Policy)	22.2.4	22.2.2	CNC Policy 22.2.4 supports fresh installation and upgrade from 1.15.x, 22.1.x, and 22.2.x to 22.2.4. For more information on installation or upgrading, see *Oracle Communications Cloud Native Core Converged Policy Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core Policy (CNC Policy)	22.2.3	22.2.3	CNC Policy 22.2.3 supports fresh installation and upgrade support from 1.15.x, 22.1.x, and 22.2.x to 22.2.3. For more information on installation or upgrading, see *Oracle Communications Cloud Native Core Converged Policy Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core Policy (CNC Policy)	22.2.2	22.2.2	CNC Policy 22.2.2 supports fresh installation and upgrade from 1.15.x, 22.1.x, and 22.2.x to 22.2.2. For more information on installation or upgrading, see *Oracle Communications Cloud Native Core Converged Policy Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core Policy (CNC Policy)	22.2.1	22.2.1	CNC Policy 22.2.1 supports fresh installation and upgrade from 1.15.x, 22.1.x, and 22.2.0 to 22.2.1. For more information on installation or upgrading, see *Oracle Communications Cloud Native Core Converged Policy Installation and Upgrade Guide*.

Table 3-1 (Cont.) Media Pack Contents for Cloud Native Core 2.22.2

Description	NF Version	ATS Version	Upgrade Supported
Oracle Communications Cloud Native Core Policy (CNC Policy)	22.2.0	22.2.0	CNC Policy 22.2.0 supports fresh installation and upgrade from 1.15.x and 22.1.x to 22.2.0. For more information on installation or upgrading, see *Oracle Communications Cloud Native Core Converged Policy Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core Service Communications Proxy (SCP)	22.2.4	22.2.4	OCSCP 22.2.4 supports fresh installation and upgrade from 1.15.x, 22.1.x, 22.2.x to 22.2.4. 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)	22.2.3	22.2.3	OCSCP 22.2.3 supports fresh installation and upgrade from 1.15.x, 22.1.x, 22.2.x to 22.2.3. 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)	22.2.2	22.2.2	OCSCP 22.2.2 supports fresh installation and upgrade from 1.15.x, 22.1.x, 22.2.x to 22.2.2. 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)	22.2.1	22.2.1	OCSCP 22.2.1 supports fresh installation and upgrade from 1.15.x, 22.1.x, 22.2.0 to 22.2.1. 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)	22.2.0	22.2.0	OCSCP 22.2.0 supports fresh installation and upgrade from 1.15.x, 22.1.x to 22.2.0. 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 2.22.2

Description	NF Version	ATS Version	Upgrade Supported
Oracle Communications Cloud Native Core Security Edge Protection Proxy (SEPP)	22.2.2	22.2.2	OCSEPPP 22.2.2 supports fresh installation and upgrade from 22.2.0 and 22.2.1 to 22.2.2. For more information, see *Oracle Communications Cloud Native Core Security Edge Protection Proxy Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core Security Edge Protection Proxy (SEPP)	22.2.1	22.2.1	OCSEPP 22.2.1 supports fresh installation and upgrade from 22.2.0 to 22.2.1. For more information on installation or upgrading, see *Oracle Communications Cloud Native Core Security Edge Protection Proxy Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core Security Edge Protection Proxy (SEPP)	22.2.0	22.2.0	OCSEPP 22.2.0 supports fresh installation only. For more information on installation, see *Oracle Communications Cloud Native Core Security Edge Protection Proxy Installation Guide.*
Oracle Communications Cloud Native Core Unified Data Repository (UDR)	22.2.2	22.2.2	OCUDR 22.2.2 supports fresh installation and upgrade from 22.1.x or 22.2.x to 22.2.2. 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)	22.2.1	22.2.1	OCUDR 22.2.1 supports fresh installation and upgrade from 22.1.x, 22.2.0 to 22.2.1. 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)	22.2.0	22.2.0	OCUDR 22.2.0 supports fresh installation and upgrade from 22.1.x to 22.2.0. 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	22.2.4	• 22.2.x • 22.1.x • 1.10.x	• 22.2.x • 22.1.x • 1.10.x	NA	• 1.10.x • 1.6.x	• 1.22.x • 1.21.x • 1.20.x	22.2.x	• 3GPP TS 23.501 • 3GPP TS 23.502 • 3GPP TS 23.503 • 3GPP TS 29.500 • 3GPP TS 29.504 • 3GPP TS 29.510 • 3GPP TS 29.507 • 3GPP TS 29.512 • 3GPP TS 29.513 • 3GPP TS 29.514 • 3GPP TS 29.519 • 3GPP TS 29.521 • 3GPP TS 29.525 • 3GPP TS 29.594 • 3GPP TS 29.214
BSF	22.2.3	• 22.2.x • 22.1.x • 1.10.x	• 22.2.x • 22.1.x • 1.10.x	NA	• 1.10.x • 1.6.x	• 1.22.x • 1.21.x • 1.20.x	22.2.x	• 3GPP TS 23.501 v16.4.0 • 3GPP TS 23.502 • 3GPP TS 23.503 • 3GPP TS 29.500 • 3GPP TS 29.504 • 3GPP TS 29.510 • 3GPP TS 29.514 • 3GPP TS 29.521 v16.5.0 • 3GPP TS 29.214
BSF	22.2.1	• 22.2.x • 22.1.x • 1.10.x	• 22.2.x • 22.1.x • 1.10.x	NA	• 1.10.x • 1.6.x	• 1.22.x • 1.21.x • 1.20.x	22.2.x	• 3GPP TS 23.501 v16.4.0 • 3GPP TS 23.502 • 3GPP TS 23.503 • 3GPP TS 29.500 • 3GPP TS 29.510 • 3GPP TS 29.513 • 3GPP TS 29.521 v16.5.0
BSF	22.2.0	• 22.2.x • 22.1.x • 1.10.x	• 22.2.x • 22.1.x • 1.10.x	NA	• 1.10.x • 1.6.x	• 1.22.x • 1.21.x • 1.20.x	22.2.x	• 3GPP TS 23.501 v16.4.0 • 3GPP TS 23.502 • 3GPP TS 23.503 • 3GPP TS 29.500 • 3GPP TS 29.510 • 3GPP TS 29.513 • 3GPP TS 29.521 v16.5.0
CNC Console	22.2.2	• 22.2.x • 22.1.x • 1.10.x	• 22.2.x • 22.1.x • 1.10.x	NA	• 1.10.x • 1.6.x	• 1.22.x • 1.21.x • 1.20.x	NA	NA

Table 3-2   (Cont.) Compliance Matrix

CNC NF	NF Version	OCCNE	DBTier	CDCS	OSO	Kubernetes	CNC Console	3GPP
CNC Console	22.2.1	• 22.2.x • 22.1.x • 1.10.x	• 22.2.x • 22.1.x • 1.10.x	NA	• 1.10.x • 1.6.x	• 1.22.x • 1.21.x • 1.20.x	NA	NA
CNC Console	22.2.0	• 22.2.x • 22.1.x • 1.10.x	• 22.2.x • 22.1.x • 1.10.x	NA	• 1.10.x • 1.6.x	• 1.22.x • 1.21.x • 1.20.x	NA	NA
CNC Policy	22.2.6	• 22.2.x • 22.1.x • 1.10.x	• 22.2.x • 22.1.x • 1.10.x	NA	• 1.10.x • 1.6.x	• 1.22.x • 1.21.x • 1.20.x	22.2.x	• 3GPP TS 23.501 • 3GPP TS 23.502 • 3GPP TS 23.503 • 3GPP TS 29.500 • 3GPP TS 29.504 • 3GPP TS 29.510 • 3GPP TS 29.507 • 3GPP TS 29.512 • 3GPP TS 29.513 • 3GPP TS 29.514 • 3GPP TS 29.519 • 3GPP TS 29.521 • 3GPP TS 29.525 • 3GPP TS 29.594 • 3GPP TS 29.214
CNC Policy	22.2.5	• 22.2.x • 22.1.x • 1.10.x	• 22.2.x • 22.1.x • 1.10.x	NA	• 1.10.x • 1.6.x	• 1.22.x • 1.21.x • 1.20.x	22.2.x	• 3GPP TS 23.501 • 3GPP TS 23.502 • 3GPP TS 23.503 • 3GPP TS 29.500 • 3GPP TS 29.504 • 3GPP TS 29.510 • 3GPP TS 29.507 • 3GPP TS 29.512 • 3GPP TS 29.513 • 3GPP TS 29.514 • 3GPP TS 29.519 • 3GPP TS 29.521 • 3GPP TS 29.525 • 3GPP TS 29.594 • 3GPP TS 29.214

Table 3-2 (Cont.) Compliance Matrix

CNC NF	NF Version	OCCNE	DBTier	CDCS	OSO	Kubernetes	CNC Console	3GPP
CNC Policy	22.2.4	• 22.2.x • 22.1.x • 1.10.x	• 22.2.x • 22.1.x • 1.10.x	NA	• 1.10.x • 1.6.x	• 1.22.x • 1.21.x • 1.20.x	22.2.x	• 3GPP TS 23.501 • 3GPP TS 23.502 • 3GPP TS 23.503 • 3GPP TS 29.500 • 3GPP TS 29.504 • 3GPP TS 29.510 • 3GPP TS 29.507 • 3GPP TS 29.512 • 3GPP TS 29.513 • 3GPP TS 29.514 • 3GPP TS 29.519 • 3GPP TS 29.521 • 3GPP TS 29.525 • 3GPP TS 29.594 • 3GPP TS 29.214

Table 3-2 (Cont.) Compliance Matrix

CNC NF	NF Version	OCCNE	DBTier	CDCS	OSO	Kubernetes	CNC Console	3GPP
CNC Policy	22.2.3	• 22.2.x • 22.1.x • 1.10.x	• 22.2.x • 22.1.x • 1.10.x	NA	• 1.10.x • 1.6.x	• 1.22.x • 1.21.x • 1.20.x	22.2.x	• 3GPP TS 23.503 v15.5.0 • 3GPP TS 29.500 v16.3.0 • 3GPP TS 23.203 v15.4.0 • 3GPP TS 29.507 v15.5.0 • 3GPP TS 29.512 v16.4.0 • 3GPP TS 29.513 v15.5.0 • 3GPP TS 29.514 v16.4.0 • 3GPP TS 29.519 v15.5.0 • 3GPP TS 29.521 v16.5.0 • 3GPP TS 29.525 v15.3.0 • 3GPP TS 29.594 v15.5.0 • 3GPP TS 29.212 v15.4.0 • 3GPP TS 29.213 v15.4.0 • 3GPP TS 29.214 v15.4.0 • 3GPP TS 29.215 v15.1.0 • 3GPP TS 29.219 v15.1.0 • 3GPP TS 29.329 v14.0.0 • 3GPP TS 29.335 v13.1.0

Table 3-2 (Cont.) Compliance Matrix

CNC NF	NF Version	OCCNE	DBTier	CDCS	OSO	Kubernetes	CNC Console	3GPP
CNC Policy	22.2.2	• 22.2.x • 22.1.x • 1.10.x	• 22.2.x • 22.1.x • 1.10.x	NA	• 1.10.x • 1.6.x	• 1.22.x • 1.21.x • 1.20.x	22.2.x	• 3GPP TS 23.503 v15.5.0 • 3GPP TS 29.500 v16.3.0 • 3GPP TS 23.203 v15.4.0 • 3GPP TS 29.507 v15.5.0 • 3GPP TS 29.512 v16.4.0 • 3GPP TS 29.513 v15.5.0 • 3GPP TS 29.514 v16.4.0 • 3GPP TS 29.519 v15.5.0 • 3GPP TS 29.521 v16.5.0 • 3GPP TS 29.525 v15.3.0 • 3GPP TS 29.594 v15.5.0 • 3GPP TS 29.212 v15.4.0 • 3GPP TS 29.213 v15.4.0 • 3GPP TS 29.214 v15.4.0 • 3GPP TS 29.215 v15.1.0 • 3GPP TS 29.219 v15.1.0 • 3GPP TS 29.329 v14.0.0 • 3GPP TS 29.335 v13.1.0

Table 3-2 (Cont.) Compliance Matrix

CNC NF	NF Version	OCCNE	DBTier	CDCS	OSO	Kubernetes	CNC Console	3GPP
CNC Policy	22.2.1	• 22.2.x • 22.1.x • 1.10.x	• 22.2.x • 22.1.x • 1.10.x	NA	• 1.10.x • 1.6.x	• 1.22.x • 1.21.x • 1.20.x	22.2.x	• 3GPP TS 23.503 v15.5.0 • 3GPP TS 29.500 v16.3.0 • 3GPP TS 23.203 v15.4.0 • 3GPP TS 29.507 v15.5.0 • 3GPP TS 29.512 v16.4.0 • 3GPP TS 29.513 v15.5.0 • 3GPP TS 29.514 v16.4.0 • 3GPP TS 29.519 v15.5.0 • 3GPP TS 29.521 v16.5.0 • 3GPP TS 29.525 v15.3.0 • 3GPP TS 29.594 v15.5.0 • 3GPP TS 29.212 v15.4.0 • 3GPP TS 29.213 v15.4.0 • 3GPP TS 29.214 v15.4.0 • 3GPP TS 29.215 v15.1.0 • 3GPP TS 29.219 v15.1.0 • 3GPP TS 29.329 v14.0.0 • 3GPP TS 29.335 v13.1.0

Table 3-2 (Cont.) Compliance Matrix

CNC NF	NF Version	OCCNE	DBTier	CDCS	OSO	Kubernetes	CNC Console	3GPP
CNC Policy	22.2.0	• 22.2.x • 22.1.x • 1.10.x	• 22.2.x • 22.1.x • 1.10.x	NA	• 1.10.x • 1.6.x	• 1.22.x • 1.21.x • 1.20.x	22.2.x	• 3GPP TS 23.503 v15.5.0 • 3GPP TS 29.500 v16.3.0 • 3GPP TS 23.203 v15.4.0 • 3GPP TS 29.507 v15.5.0 • 3GPP TS 29.512 v16.4.0 • 3GPP TS 29.513 v15.5.0 • 3GPP TS 29.514 v16.4.0 • 3GPP TS 29.519 v15.5.0 • 3GPP TS 29.521 v16.5.0 • 3GPP TS 29.525 v15.3.0 • 3GPP TS 29.594 v15.5.0 • 3GPP TS 29.212 v15.4.0 • 3GPP TS 29.213 v15.4.0 • 3GPP TS 29.214 v15.4.0 • 3GPP TS 29.215 v15.1.0 • 3GPP TS 29.219 v15.1.0 • 3GPP TS 29.329 v14.0.0 • 3GPP TS 29.335 v13.1.0
OCCNE	22.2.3	NA	22.2.x	NA	1.10.x	1.22.x	NA	NA
OCCNE	22.2.2	NA	22.2.x	NA	1.10.x	1.22.x	NA	NA
OCCNE	22.2.1	NA	22.2.x	NA	1.10.x	1.22.x	NA	NA
OCCNE	22.2.0	NA	22.2.0	NA	1.10.x	1.22.x	NA	NA
DBTier	22.2.5	22.2.x	NA	NA	1.10.x	1.22.x	NA	NA
DBTier	22.2.4	22.2.x	NA	NA	1.10.x	1.22.x	NA	NA
DBTier	22.2.3	22.2.x	NA	NA	1.10.x	1.22.x	NA	NA
DBTier	22.2.2	22.2.x	NA	NA	1.10.x	1.22.x	NA	NA
DBTier	22.2.1	22.2.x	NA	NA	1.10.x	1.22.x	NA	NA

Table 3-2 (Cont.) Compliance Matrix

CNC NF	NF Version	OCCNE	DBTier	CDCS	OSO	Kubernetes	CNC Console	3GPP
DBTier	22.2.0	22.2.0	NA	NA	1.10.x	1.22.x	NA	NA
NEF	22.2.3	• 22.2.x • 22.1.x • 1.10.x	• 22.2.x • 22.1.x • 1.10.x	NA	NA	• 1.22.x • 1.21.x • 1.20.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
NEF	22.2.2	• 22.2.x • 22.1.x • 1.10.x	• 22.2.x • 22.1.x • 1.10.x	NA	NA	• 1.22.x • 1.21.x • 1.20.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

Table 3-2 (Cont.) Compliance Matrix

CNC NF	NF Version	OCCNE	DBTier	CDCS	OSO	Kubernetes	CNC Console	3GPP
NEF	22.2.1	• 22.2.x • 22.1.x • 1.10.x	• 22.2.x • 22.1.x • 1.10.x	NA	NA	• 1.22.x • 1.21.x • 1.20.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
NEF	22.2.0	• 22.2.x • 22.1.x • 1.10.x	• 22.2.x • 22.1.x • 1.10.x	NA	NA	• 1.22.x • 1.21.x • 1.20.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
NRF	22.2.3	• 22.2.x • 22.1.x • 1.10.x	• 22.2.x • 22.1.x • 1.10.x	NA	• 1.10.x • 1.6.x	• 1.22.x • 1.21.x • 1.20.x	22.2.x	• 3GPP TS 29.510 v15.5 • 3GPP TS 29.510 v16.3.0 • 3GPP TS 29.510 v16.7

Table 3-2 (Cont.) Compliance Matrix

CNC NF	NF Version	OCCNE	DBTier	CDCS	OSO	Kubernetes	CNC Console	3GPP
NRF	22.2.2	• 22.2.x • 22.1.x • 1.10.x	• 22.2.x • 22.1.x • 1.10.x	NA	• 1.10.x • 1.6.x	• 1.22.x • 1.21.x • 1.20.x	22.2.x	• 3GPP TS 29.510 v15.5 • 3GPP TS 29.510 v16.3.0 • 3GPP TS 29.510 v16.7
NRF	22.2.1	• 22.2.x • 22.1.x • 1.10.x	• 22.2.x • 22.1.x • 1.10.x	NA	• 1.10.x • 1.6.x	• 1.22.x • 1.21.x • 1.20.x	22.2.x	• 3GPP TS 29.510 v15.5 • 3GPP TS 29.510 v16.3.0 • 3GPP TS 29.510 v16.7
NRF	22.2.0	• 22.2.x • 22.1.x • 1.10.x	• 22.2.x • 22.1.x • 1.10.x	NA	• 1.10.x • 1.6.x	• 1.22.x • 1.21.x • 1.20.x	22.2.x	• 3GPP TS 29.510 v15.5 • 3GPP TS 29.510 v16.3.0 • 3GPP TS 29.510 v16.7
NSSF	22.2.2	• 22.2.x • 22.1.x • 1.10.x	• 22.2.x • 22.1.x • 1.10.x	NA	• 22.2.x • 22.1.x • 1.10.x	• 1.22.x • 1.21.x • 1.20.x		
NSSF	22.2.1	• 22.2.x • 22.1.x • 1.10.x	• 22.2.x • 22.1.x • 1.10.x	NA	• 1.10.x • 1.6.x	• 1.22.x • 1.21.x • 1.20.x	22.2.x	• 3GPP TS 29.531 v15.5.0 • 3GPP TS 29.531 v16.5.0
NSSF	22.2.0	• 22.2.x • 22.1.x • 1.10.x	• 22.2.x • 22.1.x • 1.10.x	NA	• 1.10.x • 1.6.x	• 1.22.x • 1.21.x • 1.20.x	22.2.x	• 3GPP TS 29.531 v15.5.0 • 3GPP TS 29.531 v16.5.0
SCP	22.2.4	• 22.2.x • 22.1.x • 1.10.x	• 22.2.x • 22.1.x • 1.10.x	22.2.0	• 1.10.x • 1.6.x	• 1.22.x • 1.21.x • 1.20.x	22.2.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	22.2.3	• 22.2.x • 22.1.x • 1.10.x	• 22.2.x • 22.1.x • 1.10.x	22.2.0	• 1.10.x • 1.6.x	• 1.22.x • 1.21.x • 1.20.x	22.2.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	22.2.2	• 22.2.x • 22.1.x • 1.10.x	• 22.2.x • 22.1.x • 1.10.x	22.2.0	• 1.10.x • 1.6.x	• 1.22.x • 1.21.x • 1.20.x	22.2.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	22.2.1	• 22.2.x • 22.1.x • 1.10.x	• 22.2.x • 22.1.x • 1.10.x	22.2.0	• 1.10.x • 1.6.x	• 1.22.x • 1.21.x • 1.20.x	22.2.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	22.2.0	• 22.2.x • 22.1.x • 1.10.x	• 22.2.x • 22.1.x • 1.10.x	22.2.0	• 1.10.x • 1.6.x	• 1.22.x • 1.21.x • 1.20.x	22.2.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	22.2.2	• 22.2.x • 22.1.x • 1.10.x	• 22.2.x • 22.1.x • 1.10.x	22.2.x	NA	• 1.22.x • 1.21.x • 1.20.x	22.2.x	• 29.573 v 16.3.0
SEPP	22.2.1	• 22.2.x • 22.1.x • 1.10.x	• 22.2.x • 22.1.x • 1.10.x	22.2.0	NA	• 1.22.x • 1.21.x • 1.20.x	22.2.x	• 3GPP TS 29.573 v 16.3.0
SEPP	22.2.0	• 22.2.x • 22.1.x • 1.10.x	• 22.2.x • 22.1.x • 1.10.x	22.2.0	NA	• 1.22.x • 1.21.x • 1.20.x	22.2.x	• 3GPP TS 29.573 v 16.3.0
UDR	22.2.2	• 22.2.x • 22.1.x • 1.10.x	• 22.2.x • 22.1.x • 1.10.x	NA	• 22.2.x • 1.10.x • 1.6.x	• 1.22.x • 1.21.x • 1.20.x	22.2.x	• 3GPP TS 29.505 v15.4.0 • 3GPP TS 29.504 v16.2.0
UDR	22.2.1	• 22.2.x • 22.1.x • 1.10.x	• 22.2.x • 22.1.x • 1.10.x	NA	• 1.10.x • 1.6.x	• 1.22.x • 1.21.x • 1.20.x	22.2.x	• 3GPP TS 29.505 v15.4.0 • 3GPP TS 29.504 v16.2.0
UDR	22.2.0	• 22.2.x • 22.1.x • 1.10.x	• 22.2.x • 22.1.x • 1.10.x	NA	• 1.10.x • 1.6.x	• 1.22.x • 1.21.x • 1.20.x	22.2.x	• 3GPP TS 29.505 v15.4.0 • 3GPP TS 29.504 v16.2.0

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	NRF-Client	Perf-Info
BSF	22.2.4	22.2.11	22.2.4	22.2.4	22.2.2	22.2.4	22.2.2	22.2.11	22.2.11	22.2.2	22.2.5	22.2.4
BSF	22.2.3	22.2.7	22.2.3	22.2.3	22.2.3	22.2.3	22.2.1	22.2.7	22.2.7	22.2.1	22.2.4	22.2.3
BSF	22.2.1	22.2.7	22.2.1	22.2.0	22.2.1	22.2.1	22.2.1	22.2.7	22.2.7	22.2.1	22.2.4	22.2.1
BSF	22.2.0	22.2.4	22.2.0	22.2.0	22.2.0	22.2.0	22.2.0	22.2.4	22.2.4	22.2.0	22.2.2	22.2.0
CNC Console	22.2.2	NA	NA	NA	NA	NA	22.2.2	NA	22.2.11	22.2.2	NA	NA
CNC Console	22.2.1	NA	NA	NA	NA	NA	22.2.1	NA	22.2.6	22.2.1	NA	NA
CNC Console	22.2.0	NA	NA	NA	NA	NA	22.2.0	NA	22.2.3	22.2.0	NA	NA
CNC Policy	22.2.6	22.2.11	22.2.4	22.2.4	22.2.4	22.2.4	22.2.2	22.2.11	22.2.11	22.2.2	22.2.5	22.2.4
CNC Policy	22.2.5	22.2.11	22.2.4	22.2.4	22.2.2	22.2.4	22.2.2	22.2.11	22.2.11	22.2.2	22.2.5	22.2.4
CNC Policy	22.2.4	22.2.11	22.2.4	22.2.4	22.2.2	22.2.4	22.2.2	22.2.11	22.2.11	22.2.2	22.2.5	22.2.4
CNC Policy	22.2.3	22.2.7	22.2.3	22.2.3	22.2.3	22.2.3	22.2.1	22.2.7	22.2.7	22.2.1	22.2.4	22.2.3
CNC Policy	22.2.2	22.2.7	22.2.1	22.2.0	22.2.2	22.2.1	22.2.1	22.2.7	22.2.7	22.2.1	22.2.4	22.2.1
CNC Policy	22.2.1	22.2.7	22.2.1	22.2.0	22.2.1	22.2.1	22.2.1	22.2.7	22.2.7	22.2.1	22.2.4	22.2.1
CNC Policy	22.2.0	22.2.4	22.2.0	22.2.0	22.2.0	22.2.0	22.2.0	22.2.4	22.2.4	22.2.0	22.2.2	22.2.0
NEF	22.2.3	NA	22.2.4	NA	22.2.2	22.2.4	22.2.2	22.2.11	22.2.11	22.2.2	22.2.5	22.2.4
NEF	22.2.2	NA	22.2.4	NA	22.2.2	22.2.4	22.2.2	22.2.11	22.2.11	22.2.2	22.2.5	22.2.4
NEF	22.2.1	NA	22.2.1	NA	22.2.1	22.2.1	22.2.1	22.2.7	22.2.7	22.2.1	22.2.4	22.2.1
NEF	22.2.0	NA	22.2.0	NA	22.2.0	22.2.0	22.2.0	22.2.2	22.2.2	22.2.0	22.2.1	22.2.0
NRF	22.2.3	22.2.11	22.2.4	22.2.0	22.2.2	NA	22.2.2	22.2.11	22.2.11	22.2.2	NA	22.2.4
NRF	22.2.2	22.2.7	22.2.1	22.2.0	22.2.2	NA	22.2.2	22.2.10	22.2.10	22.2.2	NA	22.2.1
NRF	22.2.1	22.2.7	22.2.1	22.2.0	22.2.1	NA	22.2.1	22.2.7	22.2.7	22.2.1	NA	22.2.1
NRF	22.2.0	22.2.4	22.2.0	22.2.0	22.2.0	NA	22.2.0	22.2.4	22.2.4	22.2.0	NA	22.2.0
NSSF	22.2.2	NA	22.2.4	22.2.2	22.2.2	NA	22.2.0	22.2.3	22.2.3	22.2.0	22.2.1	22.2.0
NSSF	22.2.1	NA	22.2.1	22.2.1	22.2.1	NA	22.2.1	22.2.6	22.2.6	22.2.1	22.2.4	22.2.1
NSSF	22.2.0	NA	22.2.0	22.2.0	22.2.0	NA	22.2.0	22.2.3	22.2.3	22.2.0	22.2.1	22.2.0
SCP	22.2.4	NA	NA	NA	22.2.2	NA	22.2.2	NA	NA	22.2.2	NA	NA
SCP	22.2.3	NA	NA	NA	22.2.2	NA	22.2.2	NA	NA	22.2.2	NA	NA
SCP	22.2.2	NA	NA	NA	22.2.1	NA	22.2.1	NA	NA	22.2.1	NA	NA
SCP	22.2.1	NA	NA	NA	22.2.1	NA	22.2.1	NA	NA	22.2.1	NA	NA
SCP	22.2.0	NA	NA	NA	22.2.0	NA	22.2.0	NA	NA	22.2.0	NA	NA
SEPP	22.2.2	NA	22.2.4	NA	22.2.2	22.2.4	22.2.2	22.2.11	22.2.11	NA	22.2.5	22.2.4

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

CNC NF	NF Version	Alternate Route Svc	App-Info	ASM Configuration	ATS Framework	Config-Server	Debug-tool	Egress Gateway	Ingress Gateway	Helm Test	NRF-Client	Perf-Info
SEPP	22.2.1	NA	22.2.1	NA	22.2.1	22.2.1	NA	22.2.6	22.2.6	NA	22.2.4	22.2.1
SEPP	22.2.0	NA	22.2.0	NA	22.2.0	22.2.0	NA	22.2.3	22.2.3	NA	22.2.1	22.2.0
UDR	22.2.2	22.2.11	22.2.4	22.2.0	22.2.2	22.2.4	22.2.2	22.2.11	22.2.11	22.2.2	22.2.6	22.2.4
UDR	22.2.1	22.2.6	22.2.1	22.2.0	22.2.1	22.2.1	22.2.1	22.2.6	22.2.6	22.2.1	22.2.4	22.2.1
UDR	22.2.0	22.2.2	22.2.0	22.2.0	22.2.0	22.2.0	22.2.0	22.2.3	22.2.2	22.2.0	22.2.2	22.2.0

3.4 Security Certification Declaration

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

Table 3-4 Security Certification Declaration

CNC NF	NF Version	Systems test on functional and security features	Regression testing on security configuration	Vulnerability testing	Fuzz testing on external interfaces
BSF	22.2.4	October 10, 2022	October 12, 2022	October 14, 2022	October 14, 2022
BSF	22.2.3	June 20, 2022	June 24, 2022	June 24, 2022	May 27, 2022
BSF	22.2.1	June 20, 2022	June 24, 2022	June 24, 2022	May 27, 2022
BSF	22.2.0	May 16, 2022	May 16, 2022	May 16, 2022	May 03, 2022
CNC Console	22.2.2	NA (no new security features)	October 12, 2022	October 12, 2022	October 16, 2022
CNC Console	22.2.1	NA (no new security features)	May 18, 2022	June 27, 2022	May 16, 2022
CNC Console	22.2.0	NA (no new security features)	May 18, 2022	May 16, 2022	May 16, 2022
CNC Policy	22.2.6	October 10, 2022	October 12, 2022	October 14, 2022	October 14, 2022
CNC Policy	22.2.5	October 10, 2022	October 12, 2022	October 14, 2022	October 14, 2022
CNC Policy	22.2.4	October 10, 2022	October 12, 2022	October 14, 2022	October 14, 2022
CNC Policy	22.2.3	July 15, 2022	July 15, 2022	July 15, 2022	NA
CNC Policy	22.2.2	May 16, 2022	May 16, 2022	May 16, 2022	May 03, 2022
CNC Policy	22.2.1	May 16, 2022	May 16, 2022	May 16, 2022	May 03, 2022
CNC Policy	22.2.0	May 16, 2022	May 16, 2022	May 16, 2022	May 03, 2022
NEF	22.2.3	January 18, 2023	January 18, 2023	January 18, 2023	May 06, 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
NEF	22.2.2	October 4, 2022	October 4, 2022	October 4, 2022	May 06, 2022
NEF	22.2.1	July 1, 2022	July 1, 2022	July 1, 2022	May 06, 2022
NEF	22.2.0	May 13, 2022	May 06, 2022	May 13, 2022	May 06, 2022
NRF	22.2.3	October 10, 2022	October 10, 2022	October 10, 2022	October 10, 2022
NRF	22.2.2	September 20, 2022	September 20, 2022	September 20, 2022	September 20, 2022
NRF	22.2.1	July 1, 2022	July 1, 2022	July 1, 2022	May 13, 2022
NRF	22.2.0	May 13, 2022	May 13, 2022	May 13, 2022	May 13, 2022
NSSF	22.2.2	October 12, 2022	October 12, 2022	October 12, 2022	October 12, 2022
NSSF	22.2.1	June 29, 2022	June 29, 2022	June 29, 2022	June 29, 2022
NSSF	22.2.0	May 13, 2022	May 13, 2022	May 13, 2022	May 13, 2022
SCP	22.2.4	May 16, 2022	May 20, 2022	October 27, 2022	May 18, 2022
SCP	22.2.3	May 16, 2022	May 20, 2022	October 27, 2022	May 18, 2022
SCP	22.2.2	May 16, 2022	May 20, 2022	Jun 28, 2022	May 18, 2022
SCP	22.2.1	May 16, 2022	May 20, 2022	Jun 28, 2022	May 18, 2022
SCP	22.2.0	May 16, 2022	May 20, 2022	May 18, 2022	May 18, 2022
SEPP	22.2.2	October 14, 2022	October 14, 2022	NA	NA
SEPP	22.2.1	July 4, 2022	July 4, 2022	July 4, 2022	July 4, 2022
SEPP	22.2.0	May 22, 2022	May 22, 2022	May 22, 2022	May 20, 2022
UDR	22.2.2	NA (no new security features)	October 7, 2022	October 7, 2022	October 7, 2022
UDR	22.2.1	NA (no new security features)	May 20, 2022	May 20, 2022	May 20, 2022
UDR	22.2.0	NA (no new security features)	May 20, 2022	May 20, 2022	May 13, 2022

3.5 Documentation Pack

All documents for Cloud Native Core (CNC) 2.22.2 are available for download on SecureSites and MOS.

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

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

4 Resolved and Known Bugs

This chapter lists the resolved and known bugs for Cloud Native Core release 2.22.2.

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

4.1 Severity Definitions

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

Severity 1

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

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

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

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

Severity 2

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

Severity 3

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

Severity 4

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

4.2 Resolved Bug List

The following Resolved Bugs tables list the bugs that are resolved in Cloud Native Release 2.22.2.

4.2.1 BSF Resolved Bugs

BSF 22.2.4 Resolved Bugs

There are no resolved bugs in this release.

Table 4-1 BSF 22.2.3 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
34497714	Diameter Gateway is running out of memory in 22.2.0 due to peer config issues.	Diameter Gateway is running out of memory in 22.2.0 due to peer config issues.	3	22.2.0

BSF 22.2.1 Resolved Bugs

There are no resolved bugs in this release.

BSF 22.2.0 Resolved Bugs

There are no resolved bugs.

4.2.2 CNC Console Resolved Bugs

Table 4-2   CNC Console 22.2.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34598383	"cncc_vfnd.mf" file Corrections Requested	Customer indicates that the CNCC CSAR cncc_vfnd.mf file has a couple of errors that the customer has to correct before they can install the CNCC. Following changes are suggested which are taken care as part of the fix. line 5: "vnf_release_data_time" should be "vnf_release_date_time" line 6: white space should be removed.	3	22.2.1
34554147	Single Cluster Upgrade Order is incorrect in Documentation	Single Cluster Upgrade Order is incorrect in CNC Console Installation and Upgrade guide. As a fix documentation is updated.	3	22.2.1
34644132	CS_WRITE Role Mapping issues with PCF	Customer requested for a way to have CS_WRITE enabled and stop access to all Policy entries. Code changes are done to fix the issue.	3	22.1.0

Table 4-3   CNC Console 22.2.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34336763	Password of CNCC users present in CNCC pod Logs	CNCC users password was not masked in CNCC pod logs. Code changes are done to mask the password.	4	1.9.1
34322093	CNCC custom values yaml Files Image names do not match image names in build	CNCC custom values yaml files image names were not match image names in package. As a fix, package is updated with the correct image name.	4	22.2.0

Table 4-4 CNC Console 22.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34048278	ProvGW/cnUDR SOAP error	Error observed in provisioning screen when user clicks the Clear button and performs the Get operation. Code changes are made in the Console to fix the issue.	4	1.9.0
34048317	ME Lab CNCC 1.6.1: delayed logout of CCNC core portal, "Connecting to getbootstrap.com"	Log out button on click was trying to download artifacts from the internet but the button was stuck due to restricted internet access. Code changes are made for offline access of artifacts.	4	1.6.1

4.2.3 DBTier Resolved Bugs

Table 4-5 cnDBTier 22.2.5 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34757053	Helm test failed for cnDBTier after successful install	Helm test was not working when the ndbmysqld replica count is 0.	3	22.3.0
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 with error "the incident LOST_EVENTS occurred on the master. Message: mysqld startup" during a cnPCRF upgrade.	3	22.3.0

Table 4-6 cnDBTier 22.2.4 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34825292	DBTier upgrade failing from 1.15.4 to 22.2.0.	DBTier upgrade from version 1.15.4 to version 22.2.0 was failing.	2	22.2.0

Table 4-7   cnDBTier 22.2.3 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
34305187	After cnDBTier stop and start, data (ndbmtd) pods go into CrashLoopBackOff	When a cnDBTier with multiple data pods are deleted (restarted), some pods do not get restarted and go into CrashLoopBackOff.	3	22.1.0
34484443	Dual stack support for db-backup-manager-svc	The current http server of db-backup-manger-svc supports only ipv4. Therefore, db-backup-manger-svc runs only in ipv4 and dual-stack k8 cluster but not in ipv6 cluster.	3	22.2.0
34491315	Fix the manifest file in the CSAR package for cnDBTier	The variable name "vnf_release_data_time" is incorrect in the manifest file in the cnDBTier CSAR package due to which the CSAR validation is failing at the customer site.	3	22.2.1
34670991	Input cronjob expression for routine backups	The db-backup-manager-svc can only schedule routine backups based on the number of days defined in values.yaml. Consequently, the user cannot 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

Table 4-7 (Cont.) cnDBTier 22.2.3 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
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. Due to this, the non-real-time local status API is giving wrong output.	3	22.1.0
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

Table 4-8 cnDBTier 22.2.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34418396	Fix the TOSCA.meta file in the cnDBTier CDCS CSAR Template	The "`TOSCA-Metadata/TOSCA.meta`" file had incorrect entry for '`Entry-Definitions`' and '`ETSI-Entry-Manifest`' attributes.	3	22.2.1

Table 4-9 cnDBTier 22.2.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34308261	Use latest Ol8+JDK base image OL85s220614|JDK17.0.3.1 in all cnDBTier k8 services	The OL85s220614|JDK17.0.3.1 docker image must be used for DB Tier Kubernetes services running on JVM (that is, db-monitor-svc and db-replication-svc).	3	22.2.0
34308341	Allowing the Disaster recovery of cnDBTier clusters even if the cluster2 and cluster3 is getting reinstalled without cluster1	Automated disaster recovery is stuck in the initial state and it is triggered again if cnDBTier cluster2 and cnDBTier cluster3 are installed as mated pairs without installing the cnDBTier cluster1.	3	22.2.0
34213452	Error=Failed getting connection; pool exhausted in db backup svc	If the disaster recovery is being performed multiple times, the connection between the database and the backup service is denied, as the connection pool gets exhausted.	3	22.2.0

Table 4-9 (Cont.) cnDBTier 22.2.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34308634	Removing the extra directory during creation of CDCS compatible cnDBTier CSAR file	cnDBTier CDCS CSAR package has one extra top level directory that must be removed.	3	22.2.0
34308412	Fix the CI/CD pipeline to upload the checksum file in correct format	The build containing the CSAR package and checksum file are uploaded to the cnDBTier Artifact hub. The format of the checksum file is getting changed in the Artifact hub.	3	22.2.0
34308439	cnDBTier helm test uses deployment name to grep for pod name	cnDBTier helm test fails if db-replication-svc deployment name is longer than 58 characters.	3	22.2.1
34327850	1.10.3 to 22.1 cnDBTier upgrade (without ServiceAccount) is failing	cnDBTier upgrade fails as helm does not have permission to list events and therefore is not able to run the pre and post-upgrade hook correctly.	3	22.1.1
34269846	cnDBTier helm test fails checking db-replication-svc pod is on ASM clusters	To determine if db-replication-svc pods are READY state, the test script checks if the number of containers that are in READY state are equal to the number of containers in the pod.	4	22.2.0

Table 4-10 cnDBTier 22.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34084036	cnDBTier mysqld livenessProbes causes MySQL connect errors	On opening a TCP connection, cnDBTier mysqld livenessProbe causes MySQL connect errors and it is closed without properly logging into mysql.	2	1.10.1

4.2.4 CNC Policy Resolved Bugs

Table 4-11 CNC Policy 22.2.6 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
34811446	IP Can Session Termination Blockly Not working	When sending RX STR (GX/RX sessions only with ipv6) and triggering the release of all PCEF/TDF sessions associated with the IP CAN session, an internal null pointer exception occurs.	2	22.2.0
34931745	PolicyDS PCRF-CORE-DELETE above threshold	PDS was being contacted on a DELETE request every time without validating the advanced settings to check if it should contact PDS.	3	22.2.0
34536350	STR Returned with Diameter Unknown Session ID-5002	PCRF-Core is not responding to some ASRs due to the deletion of the session.	3	1.15.4
35018232	PCRF-Core not responding to some ASRs due to deleting the session twice	PCRF is not deleting the Rx session from the cache when the DB session is deleted. When a message arrives it finds the session and processes it. But when it tries to insert the DB, it does not find the record and the delivery fails.	4	22.3.0

Table 4-12   CNC Policy 22.2.5 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
34842441	Sy Data source Redundancy is not working for 22.2.3	Inter-Pod Routing in diameter-gateway is not handled, when multiple Sy-DSR interfaces are configured and if one of the available Sy-DSR interface goes down.	2	22.2.3
34811446	IP Can Session Termination Blockly Not working	Policy Action blockly "Release all PCEF/TDF session associated with IP-CAN Session" is not working for AAR, if the IPv6 prefix length used is different in CCR-I and AAR.	2	22.2.0
34867936	SPAD_POLICY In-service upgrade for cnPCRF failed for 10M active subscriber	If DB has lot of records and the upgrade path requires table conversion, then additional time is needed for upgrade depending upon the number of records.	2	22.4.0
34644934	PCF:BT:PCRF core rejecting the traffic with diameter authorization rejected with 5003	When the requests are received from unauthorized PGWs, they are rejected with diameter error code(5003).	3	1.15.0

Table 4-13 CNC Policy 22.2.4 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
34677029	Increase of PCF 404 Errors - Need Audit Timer change for issue found in 22.2.3 after upgrade	The validity of the PDS session with core service used to be a synchronous call. It was upgraded to be an asynchronous call but the asynchronous call session is getting declared stale even before the asynchronous call is complete, leading to inconsistent behavior.	2	22.2.3

CNC Policy 22.2.3 Resolved Bugs

Table 4-14 CNC Policy 22.2.3 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
34387482	PCF is not sending timestamp headers to nbsf even if all configuration mentioned in the Installation and User Guide is followed.	PCF is not sending timestamp headers to nbsf even if all configuration mentioned in the Installation and User Guide is followed.	2	22.2.1
34497756	If there are any timer configuration change in CNC Console audit settings, PDS pod restarts.	If there are any timer configuration change in CNC Console audit settings, PDS pod restarts.	2	22.2.1
34355577	PCF does not install session and PCC rules for an Emergency 911 call for an unknown user.	PCF does not install session and PCC rules for an Emergency 911 call for an unknown user.	2	22.2.0

Table 4-14 (Cont.) CNC Policy 22.2.3 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
34497684	Diameter Gateway leaks ReconnectWaitThread when the outgoing peer is down.	Diameter Gateway leaks ReconnectWaitThread when the outgoing peer is down.	3	1.15.1
34511972	When the late arrival is detected, sm-service logs does not show 504 response sent to SMF.	When the late arrival is detected, sm-service logs does not show 504 response sent to SMF.	3	22.1.2
34512000	Session information is not synchronized with SMF due to PCF Gateway timeout.	Session information is not synchronized with SMF due to PCF Gateway timeout.	3	22.1.2
34512012	PCF fails to terminate N7 session for a SIMless SOS call.	PCF fails to terminate N7 session for a SIMless SOS call.	3	22.1.2
34512052	PCF Upgrade to 22.2.1 fails and causes db replication errors.	PCF Upgrade to 22.2.1 fails and causes db replication errors.	3	22.1.2

Table 4-15 CNC Policy 22.2.3 ATS Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
34497735	PCF ATS testcase, Topology_hiding_SM_Rx_for_STR&AAR, is failing.	PCF ATS testcase, Topology_hiding_SM_Rx_for_STR&AAR, is failing.	3	22.2.1

CNC Policy 22.2.2 Resolved Bugs

Table 4-16 CNC Policy 22.2.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
34374603	Missing SuppFeat in UE policy 201 Created message	Missing SuppFeat in UE policy 201 Created message and setting SuppFeat IE	3	22.1.2

Table 4-16 (Cont.) CNC Policy 22.2.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
34391389	nCHF DELETE right after successful nCHF PUT	PCF is sending nCHF DELETE right after successful nCHF PUT.	3	22.1.2

CNC Policy 22.2.1 Resolved Bugs

Table 4-17 CNC Policy 22.2.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
34306376	POLICY_GENERIC Multiple issues in Policy User Guide for 22.2. 0		4	22.2.0
34122498	PDS Stale Data Improvement - Revalidation		3	22.2.0
34335891	Pending Transaction and Retries		3	22.1.2
34297983	POLICY_BULWARK PCRF-Core set lockWaitTimeout as Zero for CCR-U to bulwark for lock		3	22.2.0
34282410	POLICY_BULWARK PCRF-Core sent CCR-I success even after LOCK_REQUEST_RETRY_COUNT_FOR_CREATE exhausted for this session		3	22.2.0
34337819	PCRF-Core is not attempting for polling lock state based on LOCK_WAIT_DURATION_FOR_CREATE for multiple CCR-I		3	22.2.0
34282432	POLICY_BULWARK No Bulwark lock initiated for CCR-T with default configuration on 22.2.0		2	22.2.0
34282375	PI-D to PI-A upgrade failed due to bsf-mgmt post upgrade hook pod timing out		2	22.1.3
34337830	nUDR PUT getting 403 Forbidden response from UDR		3	22.2.0

Table 4-17   (Cont.) CNC Policy 22.2.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
34262671	PCF |22.2.0 | Server Header Retry Not Working for GET Request (Towards UDR) | CNCES-6363		3	22.2.0
34337837	ATS: NetLoc_on_N7 feature fails at validation of Diameter Gateway logs		3	22.2.0
34335788	ATS: UE_N1N2_SubscribeAltRoute_Exclude_SH_Instance sceanrio of UE_NAS_SessRetry feature fails		3	22.2.0
34335900	PCF 22.1.2 Pending transaction on reauth w/ 500 error caused SMF update 504 timeout		3	22.1.2
34335732	nrf-client-nfmanagement occasionally sends REGISTERED to NRF when appinfo indicates PCF down		3	22.2.0
34335422	PCF PDS PROFILE TABLE with pds_profile_id duplicates- with few same SUPI/GPSI and NULL site_id		3	22.2.0
34335389	chf-connector pod returning 500 error for No CHF DataSource found		3	22.2.0
34282515	CNCES-6081 VzW PCF: PCF 22.1.2 No UDR retry attempt on SM create if "Enable Discovery On Demand" is true		3	22.1.0

Table 4-18   CNC Policy 22.2.1 ATS Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
34122608	ATS SM notify contains null attributes under SM Policy Decisions in PI-A	ATS SM notify contains null attibutes under SM Policy Decisions	3	22.1.0

CNC Policy 22.2.0 Resolved Bugs

Table 4-19 CNC Policy 22.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
33904374	LDAP traffic stops being reported when SSV is enabled.	When SSV is enabled, LDAP traffic stops.	3	22.1.0
33904441	Policy UI sometimes allows Model D with discovery parameter as TARGET_NF_SET_ID and some other anomalies as well	In the Add Initial discovery parameter window, when CLOSE button is clicked, then PARAM NAME drop down is not getting refreshed.	3	22.1.0
33904838	PCF_22.1.0_RC_ATS_test_case_failing-Pcrf_core_audit	PCRF Core Audit test cases in Converged mode is failing in ATS execution.	3	22.1.0

4.2.5 CNE Resolved Bugs

Table 4-20 CNE 22.2.3 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
34931418	Validation tests are failing during installation of 22.4.0 GA	The validation tests failed during the testing phase while installing OCCNE 22.4.0.	4	22.4.0
34943010	Installation failing due to coredns test.	The validation tests failed during the testing phase while installing OCCNE 22.4.0.	4	22.4.0
34815972	NEW X9-2 SERVERS CONFIGURATION	Server configuration was required for the new X9-2 servers in the customer's labs as the configuration for the new servers was different from the existing X8-2 servers.	4	22.4.0

Table 4-21 CNE 22.2.2 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 working. This bug impacts all hosts or VMs of the 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

Table 4-22 CNE 22.2.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34218372	vCNE 22.2.0 on VMware validation is incomplete	Validation of OCCNE 22.2.x is incomplete for vCNE on VMware. Customers using vCNE on VMware are advised to not use OCCNE 22.2.0 for fresh install or upgrade.	3	22.2.0

Table 4-23 CNE 22.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34185501	Add 'dnf update' when using OL8-slim image from Oracle repository	When building OCCNE container images, they have latest Oracle Linux errata packages and resulting image does not have security CVEs.	2	22.1.0
34186091	ToR switch edge ports need edge trunk for trunk mode ports.	When installing 22.1.0 on odyssey cluster, PXE boot failed for all RMS servers. They cannot get DHCP addresses while the blade servers can.	3	22.1.0

Table 4-23 (Cont.) CNE 22.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34186312	Fix Grafana alert expression	Grafana's alert expression stopped working due to a change in the metrics attribute. When Grafana app is down, there is no alert raised.	3	22.1.0
34186200	Kubectl event SyncLoadBalancerFailed is reported for LoadBalancer resources	The Kubernetes reports SyncLoadBalancerFailed events for the LoadBalancer resources from CNE 1.9 onwards.	3	22.1.0
34186335	The deploy.sh script doesn't have error message for name_server missing.	The deploy.sh stopped after completing the host server installation without an error message, but failed with the bastion host creation. When running the podman command on bastion host only, the error "name_server not in ansible variable" was displayed.	3	22.1.0
34186364	Missing images in file K8S_containner_images.txt available in occne_dependencies.tar.gz	Openstack environment dependent images are missing in the file K8S_contianer_images.txt available in occne_dependencies.tar.gz.	3	22.1.0
34186162	DB Tier install image included in OC-CNE dependency list	DBTier image listed as OC-CNE dependency does not exist.	4	22.1.0

4.2.6 NEF Resolved Bugs

OCNEF Release 22.2.3

Table 4-24 OCNEF 22.2.3 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
34918982	NEF throwing 400 Bad Request to Monitoring event	NEF subscription RefId is made configurable with default value as 32 bit unsigned.	2	22.2.2

OCNEF Release 22.2.2

There are no resolved bugs in NEF Release 22.2.2.

OCNEF Release 22.2.1

There are no resolved bugs in NEF Release 22.2.1.

OCNEF Release 22.2.0

There are no resolved bugs in NEF Release 22.2.0.

4.2.7 NRF Resolved Bugs

NRF 22.2.3 Resolved Bugs

There are no resolved bugs in NRF Release 22.2.3.

Table 4-25 NRF 22.2.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
34616372	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
34556717	NRF R16 ServiceMap feature - Error code 400 for Heartbeat request after Upgrade from 22.1.0 to 22.2.0	Heartbeat Request getting Error code 400 (BAD Request) after upgrade.	3	22.2.0
34611851	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
34617157	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	4	22.1.0
34617171	NRF Istio-logs contain unexpected dashes	maxLifetime parameter value is lesser than hikariIdleTimeout value.	4	1.15.1

Table 4-25 (Cont.) NRF 22.2.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
34617139	Westlake ATS is failing on the regression test. Update systemOptions_cleanup.sh script provided as part of ATS for nfAccessTokenOptions and validate other configurations	Update systemOptions_cleanup.sh script provided as part of ATS for nfAccessTokenOptions and validate other configurations.	4	1.15.0
34617190	"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
34617266	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	4	22.2.0
34617291	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
34617372	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-apirootRight now OCNRF is not appending '0' in 2-digit MNC to make it as 3 digits.*	3	22.1.0
34617501	NFServiceList: NFServices and NFServiceList both are not working vice-versa randomly when Patch is applied on Service level attribute.	NFServices and NFServiceList both are notworking vice-versa randomly.	3	22.2.0
34617517	Updates Requested In CSAR MF File	Updates requested In CSAR MF File has special characters such as spaces and tabs.	3	22.2.0
34617542	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

Table 4-25 (Cont.) NRF 22.2.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
34618759	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
34618743	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
34618732	Troubleshooting: Add support for printing X-REQUEST-ID generated by Istio sidecar in all of the application logs	Added support for printing X-REQUEST-ID generated by Istio sidecar in all of the application logs	4	22.2.0
34618696	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

NRF 22.2.1 Resolved Bugs

Table 4-26 NRF 22.2.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
34341433	NFSubscription logs need details for Duplicate Subscriptions	NF Subscription logs are not printing the duplicate subscription details. While troubleshooting not able to find which subscription is duplicate along with the details.	4	22.1.0

NRF 22.2.0 Resolved Bugs

Table 4-27 NRF 22.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
33968318	NRF not maintaining EgressGw route config after helm upgrade, setting it to default config.	During upgrade from 1.15.x to 22.1.0, NRF is resetting all the EGW SBI route configurations to default route. Hence, if any SBI Route is configured in EGW, after upgrade, all the Egress Traffic will only use Direct Route, not SBI Route based routing which may result into failure.	2	22.1.0
34084841	NRF to secondary SEPP routing for discovery request not working	Scenario: NRF routing to secondary SEPP if primary not available. Steps:- Create dummy SEPP as primary SEPP in EGW config Create real SEPP as secondary SEPP in EGW config Send inter plmn discovery request to NRFResult: NRF responds with 500 and does not attempt to secondary SEPP.	2	22.1.0
34208288	OCNRF microservices pods threads getting killed randomly	NRF microservice pods threads getting killed randomly. Impact:- NRF some of the functionality like Management services, replication service will be impacted.	2	22.1.0
34199938	Lowering "averageCpuUtil" for triggering HPA for NfDiscovery and NfAccessToken services.	The CPU threshold "averageCpuUtil" for triggering HPA needs to be set to a lower value for NfDiscovery and NfAccessToken services so that when HPA raises in the existing PODs have enough space available to absorb the spike in traffic until the new pod is ready.	3	22.1.0

Table 4-27 (Cont.) NRF 22.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
34199979	AMF registration is failing when amfInfo.n2InterfaceAmfInfo has only ipv6Addresses.	When a registration request is sent to NRF to register an AMF with only ipv6Addresses in amfInfo.n2InterfaceAmfInfo, the registration is failing with 500 response code response body:- `{"title":"Internal Server Error","status":500,"detail":"Internal Error during database access","cause":"UNSPECIFIED_NF_FAILURE"}`	3	1.15.0
34128407	Update User Doc to indicate usage of the User-Agent header to identify the requester nfType in Roaming Scenario	Considering the scenario where the requester nfType is not available, it is assumed that the traffic is a roaming OUT case with a token request for a specific producer (request done with targetNfInstanceId). For non roaming out case if the nfType is not given in the request the nfType is retrieved from the registered nfProfile of the requester nf in the NRF.	4	22.1.0

Table 4-27 (Cont.) NRF 22.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
34086430	NRF- SLF Discovered Candidate List is still populated even after "populateSlfCandidateList": false for feature NRF-SLFQuery via SCP	Once set parameter "populateSlfCandidateList": true and reset to "populateSlfCandidateList": false, "slfDiscoveredCandidateList" is still getting populated with Registered SLF.Expectation: "slfDiscoveredCandidateList" parameter should not get populated with Registered SLFs.	4	22.1.0
34138319	Correction required in "current" spelling observed in registration pod logs	Correction required in "current" spelling observed in registration pod logs	4	22.1.0
34191511	CSAR ocnrf_vnfd.yml file contains additional "tab" which may cause issue	A TAB character in the vnfd file of the CSAR package may cause issue during installation by the Orchestrator. This needs to be removed.	4	22.1.0
34199964	Remove multiple servicePorts sections under global section in umbrella values.yaml	In global section of NRF's umbrella values.yaml, two instance of servicePorts section are added, one for appinfo and perfinfo sections. This is resulting into only one of them getting picked by Helm, not merging it.	4	22.1.2

4.2.8 NSSF Resolved Bugs

Table 4-28 NSSF 22.2.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34646256	Backup Configuration not working on NSSF	NSSF config back up API is responding with an error when the AMF set is not configured.	3	22.2.1

Table 4-28 (Cont.) NSSF 22.2.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34646255	OC_Notify is getting added in POST notification message	OC_Notify is getting added to POST notification message	3	22.2.1
34646498	NSSF is responding with 5XX return code for GET API for network-slice-information without TAI	NSSF is responding with a 5XX return code for GET API for network-slice-information without TAI. NSSF must respond with 400 Bad requests and mention that the Conditional param TAI is missing.	3	22.2.0

NSSF 22.2.1 Resolved Bugs

There are no resolved bugs in this release.

NSSF 22.2.0 Resolved Bugs

Table 4-29 NSSF 22.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34122264	NSSF is answering 200 OK to POST nssai-availability subscriptions instead of 201	Instead of 201, NSSF is responding with 200 OK while sending a POST request for nssai-availability subscriptions.	2	22.1.0
34141597	NSSAIAvailability scenario NSSF does not provide AMF with the right information	NSSAIAvailability scenario in NSSF does not provide AMF with the right information.	3	22.1.0
34141657	NSSF responds for Availability Update with TacRanges to AMF which does not support ONSSAI	In a NSSAIAvailability scenario, if ONSSAI feature is enabled, taiRangeList is provided regardless of receiving "supportedFeatures": "0".	3	22.1.0
34119541	Data too long for column service_name	Data is too long for column service_name.	3	22.1.0

4.2.9 SCP Resolved Bugs

Table 4-30 SCP 22.2.4 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35183327	SCP sending 503 due to Circuit Breaking condition not clearing.	Total transaction timeout on SCP resulted in Circuit Breaking count with stale values causing some traffic failures in SCP.	2	22.2.2
35183347	SCP R15 reverse proxy rules get deleted and are not safeguarded when parallel processing of profiles from configuration module (SCP and NRF).	SCP R15 reverse proxy rules get removed and are not protected when concurrently processing profiles from configuration module (SCP and NRF).	2	22.2.2
34880875	SCP intermittently fails to forward NF Deregistration notification request to AMF	TCP retransmissions were observed due to peer not responding with TCP Acknowledgment. Added instrumentation to help in getting more data for debugging.	3	22.2.2
35065094	SCP does not peg metric "ocscp_failure_processed_nf_notification_total" in multiple cases and hence the dependent alert based on this metric.	SCP does not peg the ocscp_failure_processed_nf_notification_total metric in multiple scenarios.	3	22.2.2
35113063	Prometheus restart observed due to high number of samples.	Enable or disable dimensions, such as ocscp_nf_instance_id and ocscp_service_instance_id , as configurable.	3	22.2.2

Table 4-31 SCP 22.2.3 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34701947	Inter SCP notification routing not working when request URI is missing service name	Inter SCP notification routing is not working when the request URI is missing the service name and is taking a forward route to the NF producer.	2	22.1.2
34657312	"ocscp_notification_foreign_nf_locality_unserved" metric is not decrementing	"ocscp_notification_foreign_nf_locality_unserved" is pegged when an NF registers with a locality not served by any SCP but is not cleared when the NF deregisters.	3	22.1.2

Table 4-32 SCP 22.2.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34536019	SCP Frequently Subscribing and Unsubscribing to NRF over TLS	SCP is picking up incorrect port for https and therefore detecting change in NRF ipendpoint for callback URI. This issue was causing SCP to frequently subscribe and unsubscribe to NRF over TLS.	2	22.1.2
34335985	Update of SUPI range in NFprofile is not reflecting properly on SCP	SCP Notification module was not able to process the SUPI range addition to the existing NF profiles when the number of profiles are high. Optimized notification processing to fix the issue.	2	1.9.3
34547044	ATS code enhancement for timeout exception	Exception was not traced in case of request timeout on ATS. Added code to trace the exception.	3	22.2.1
34495184	Disable locality sync up for R15	scp-worker was synchronizing with locality data from notification module which is not applicable to R15 and resulting in increase in connections and memory build up on notification module.	3	22.2.1
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. Corrections are made not to process existing profiles again.	3	22.2.0
34499261	Egress Rate Limit feature throwing 503's and Circuit Breaking triggered	Circuit breaking was getting triggered in case of egress rate limiting. The pending request count was not correctly decremented in case of egress rate limiting, resulting into the issue.	3	22.2.1
34275033	SCP is not rerouting when 307 response with retry-after header is received from producer NF	SCP was not performing alternate routing when the retry-after header is received with response code 307 with producer NF.	3	1.15.3
34335955	SCP is not able to route NF notification request from NRF with https signalling port	SCP-worker was not forwarding notification requests received with https port to notification module.	3	22.1.2

Table 4-32 (Cont.) SCP 22.2.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34498881	scp_vnfd.mf corrections for blank space and typos	vnf_release_data_time is changed to vnf_release_date_time and the blank space is removed from scp_vnfd.mf file in the csar package.	4	22.1.2
34336001	ocscp_metric_routing_attempt_fail_total is not pegged correctly	Routing attempt failed metrics was getting pegged for producer error response.	4	1.15.4

Table 4-33 SCP 22.2.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34327031	Error logs while Login to ATS GUI console	Error was observed login to ATS GUI when persistent volume with data from old release is used.	3	22.1.2
34326927	Fix Notification service SSE client duplicate init and Log level change from DEBUG to Error for SSEClient Code	Fix Notification service SSE client duplicate init and Log level change from DEBUG to Error for SSEClient Code	3	22.1.2
34249989	Configuration module restart observed when scp-worker pod replica scaled to 0	Scaling scp-worker replica down and then up results in configuration module restart	3	1.15.3
34263913	Nodeport value hardcoded for mediation service in SCP deployment	Mediation charts were using node port, mediation charts are updated to use cluster IP.	3	22.2.0

Table 4-34 SCP 22.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34037558	SCP add its own Header in ServerHeader while failure (error 500) received from producer NF (NRF)	SCP was adding its own server header when forwarding error response received from NRF for delegated discovery which it should not add.	2	22.1.0
34177970	Registration With NRF Failure After deployment	SCP PLMN Id in deployment file ocscp_values.yaml is not properly read. That has been corrected and reformatted.	3	22.1.0

Table 4-34 (Cont.) SCP 22.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34177995	Enhanced_NF_Status_Processing_UNDISCOVERABLE.feature cleanup is not complete	Cleanup was not deleting the profiles configured during test. Cleanup steps are added to fix the issue.	3	22.1.2
34189588	SCP sending 404 Routing rule not found	SCP not able to extract message type when multiple parameters are there in dataset-names in ingres request URI.	3	1.15.3
34189601	'ocscp_no_nf_instance' metric is not pegging	The ocscp_no_nf_instance metric does not show in Prometheus and corresponding alerts are not triggered.	3	1.15.3
34134135	SCP is not applying SBI rules correctly on service request contain discovery headers	SCP was not applying SBI message priority rules correctly in case of delegated discovery use cases.	3	22.1.0
34107190	SCP is not creating R16 routing rules if NF profile is received with regex in Supi	With the R16 profile, if xxInfo, such as udmInfo, ausfInfo, and so on, is forwarded with a pattern, SCP invalidated it, however, SCP should not invalidate it because, in R16, SCP does not rely on xxInfo for routing decisions.	3	1.15.0
34080905	Debug image repo is not picked up from global repo variable defined in deployment file	Absolute DockerRepository path appended as prefix was missing form the ocscp_values.yaml file for debug container.	3	22.1.0
34030648	NF re-selection not working for intra plmn scenario	In case, Target-apiroot is not reachable and NF profile is present in NRF while selecting alternate route, SCP is picking up the wrong port from target api-root which it already has tried with. Instead, it should pick port from the learnt profile.	3	22.1.0
34019717	Content-Type is not set to application/problem+json in erroneous response	Content-Type is not set to application/problem+json in erroneous response.	4	22.1.0
33984407	SEPP-info with invalid nfInstanceId is allowed to be created	SEPP-info with invalid nfInstanceId is allowed to be created.	4	22.1.0

Table 4-34 (Cont.) SCP 22.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
33968724	Incorrect string value "Destionation Client Response TimeOut" in 504 Gateway Timeout response from SCP	Incorrect string value "Destionation Client Response TimeOut" in 504 Gateway Timeout response from SCP.	4	22.1.0
33933197	Update SCPIngressTrafficRate Alerts expression to add scpfqdn and scpauthority	SCPIngressTrafficRate Alerts expression to have scpfqdn and scpauthority.	4	22.1.0
33791917	ATS Documentation is not generated correctly from doxygen comments	ATS Documentation is not generated correctly from doxygen comments.	4	22.1.0
34183618	Continuous Error Logs with "in exception block null" is written in worker logs during SCP performance run	Continuous Error Logs with "in exception block null" is written in worker logs during SCP performance run. This is happening for the requests that are getting discarded silently due to CPU congestion control.	4	22.1.2
34178268	SCPAuditEmptyNFArrayResponse alert expression not correct	Metric name in SCPAuditEmptyNFArrayResponse alert expression is incorrect.	4	22.1.0
34173852	Worker_Pod_Overload_Ctrl_Policy API feature failing intemittently	Continous configuration steps were resulting in intemittent faiures. Wait time is added in testcase to avoid the condition.	4	22.1.0
34173462	SCPProducerOverloadAlternateRoute Alert field needs to be corrected	Alert name is incorrect in alert rules file (scp-alerting-rules-promha_22.1.2-beta.22.yaml).	4	22.1.0
34128238	Instruction to patch alternate resolution deployment with ATS DNS stub server config to be corrected	Instruction to patch alternate resolution deployment with ATS DNS stub server config to be corrected.	4	22.1.1
34046707	Cosmetic erors in logs	Cosmetic error in logs were reported and fixed.	4	22.1.0
33984413	PATCH for SEPPInfo is being responded with 405	PATCH request to update the ports for http and https in SEPP info is being responded with Error Code 405.	4	22.1.0
34030619	REST Specification correction required in table 2-21 and 2-22	Corrected the resource URI names in the NF Topology Groups REST API.	4	22.1.0

Table 4-34 (Cont.) SCP 22.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34030663	SCP compliance matrix 29500 6.10.8.2 need be updated from FC to PC	As per SCP compliance matrix, 3GPP 29500 section 6.10.8.2 has been marked as "FC", whereas the error response is not fully compliant.	4	22.1.0
34046720	Steps mentioned in "SCP_Installation_and_Upgrade_Guide.pdf" doc for "drop table ReleaseConfig;"	Creating wrong databse in the MySQL db.	4	1.15.0
34046726	Uninstalling SCP in "SCP_Installation_and_Upgrade_Guide.pdf" doesn't cater to drop all tables created by SCP-NF	Updated the drop database ocscpdb while upgrading SCP.	4	1.15.0
34072674	SCP auditinterval default value is not as per installation guide	Updated the SCP audit interval default value in the document.	4	22.1.0

4.2.10 SEPP Resolved Bugs

SEPP 22.2.2 Resolved Bugs

There are no resolved bugs in this release.

Table 4-35 SEPP 22.2.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34277507	SEPP 22.2.0 does not contains "Debug Tool Image".	Debug tool image was missed in SEPP 22.2.0 package delivered. Due to this issue, debug-tool container was failing. Debug-tool image is added in SEPP 22.2.1 package.	3	22.2.0
34277575	Priority field is not available for Remote SEPP form in CNC Console	CNC Console was not showing 'priority' field on New or Edit screen, however the field is present in User guide. REST API guide was up to date and priority field was not present there. Updated the User guide and removed the priority field as it is no longer used in Remote Sepp command.	4	22.2.0

Table 4-35 (Cont.) SEPP 22.2.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34302200	SEPP Installation guide updates for nrf-client configuration parameters	New parameter 'enablePDBSupport' was added by NRF-Client in 22.2.0 release. This parameter details are not added installation guide. Added the parameter details in installation guide.	4	22.2.0
34302200	Warning message appears while running helm install for SEPP	While running helm install, some warnings were appearing from nrf-client charts. This is because 'core_services' present in values.yaml was defined as local list, however it should be defined as global list. Updated to define it as a global list.	4	22.2.0
34302200	Remote SEPP Editable fields need to be corrected in User Guide	Three parameters mentioned in User guide for Remote Sepp command was not in sync with REST API guide. Corrected the both guides in sync for these parameters.	4	22.2.0

Table 4-36 SEPP 22.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
3420461	SEPP on AWS Load Balancer IP not assigned to the Config-Mgr Service	Due to an incorrect loadbalancer annotation inconfig-mgr-svc, Load Balancer IP i not assigned to config-mgr-svc in AWS. Corrected the annotation and formatting issue in HELM.	2	22.1.0
33984312	No REST API to change the log level of NRF related pods for SEPP	REST API to manage log level of NRF related pods like discovery and nf-management were not exposed in SEPP.	4	22.1.0
34174693	Add removeUnusedProxyAfter in SEPP configuration guide	Added documentation for removeUnusedProxyAfter in SEPP User guide.	4	22.1.0
34108777	SEPP installation and user guide improvement points	Added the priority field in SEPP custom yaml for NRF registration. Updated the SEPP documents.	4	22.1.0

4.2.11 UDR Resolved Bugs

UDR Release 22.2.2

Table 4-37 UDR 22.2.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34646378	Prometheus_Scenarios.feature Test case Nrf_Client_Metrics_01 failed once during the ATS Regression run	During ATS Regression Run, Prometheus_Scenarios.feature Test case Nrf_Client_Metrics_01 failed once.	3	22.2.1

UDR Release 22.2.1

Table 4-38 UDR 22.2.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
SR-3-29709747751	VZW ME LAB: SLF 22.1.1 ProvGW Auditor Enabled / Large No of "OcudrSubscriberNotFoundAbove50Percent"	Need changes required in SLF_Alertrules_old.yaml for subscriber not found. Resolution: Updated the Alert file with correct metrics.	4	22.1.1
SR: 3-29763249271	SLF-CSAR Package-p34124422_116000_Tekelec- udr-nfvd.yaml is having path mismatch	There is a patch mismatch in the SLF-CSAR Package-p34124422_116000_Tekelec- udr-nfvd.yaml file. Resolution: Updated the CSAR with correct information.	4	22.1.1
SR 3-29890714681	SLF ATS 22.2.0_ProvGW All test cases	ProvGateway test failed with cleanup issues. Resolution: Fixed the ATS feature file for the issue	4	22.2.0
SR: 3-29897851741	SLF ATS 22.2.0_AlertRules_Failures	Changes required in SLF ATS 22.2.0_AlertRules.yaml for subscriber not found. Resolution: Updated the Alert file with correct metrics.	4	22.2.0

UDR Release 22.2.0

Table 4-39   UDR 22.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
30774755	Headers for few resources are not implemented as per spec 29505-v15.4.0	Headers including Cache-Control, ETag, and Last-Modified are not sent by UDR upon a successful GET request for multiple resources.	3	1.4.0
34047628	PCF |22.1.0 | PCF is not able to process the request, Getting Parsing Error for UE Policy Flow towards UDR	Parsing errors are observed on PCF-UDR-Connector for PCF to UDR of UE-Policy flow.	3	22.1.0
30774742	UDR is not validating the conditional attributes for UDM APIs	It is observed that UDR does not validate if the conditional attributes are present in the data blob based on their dependencies.	4	1.3.0

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 22.2.4 Known Bugs

There are no new known bugs.

BSF 22.2.3 Known Bugs

There are no new known bugs.

BSF 22.2.1 Known Bugs

There are no new known bugs.

BSF 22.2.0 Known Bugs

There are no new known bugs.

4.3.2 DBTier Known Bugs

DBTier Release 22.2.5

There are no new known bugs in this release.

DBTier Release 22.2.4

There are no new known bugs in this release.

DBTier Release 22.2.3

There are no new known bugs in this release.

DBTier Release 22.2.2

There are no new known bugs in this release.

DBTier Release 22.2.1

Table 4-40 DBTier 22.2.1 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
34305187	After cnDBTier stop and start, data (ndbmtd) pods go into CrashLoopBackOff	NDB MySQL Cluster never comes up, as not all of the data (ndbmtd) pods start.	NDB MySQL Cluster does not comes up. **Workaround**: Set an appropriate StartPartialTimeout value in the `[custom_]values.yaml` file for a cluster before installing cnDBTier. To stop and start the cnDBTier clusters with a large number of data pods, see *Oracle Communications Cloud Native Core DBTier User Guide*.	3	22.1.2

DBTier Release 22.2.0

Table 4-41   DBTier 22.2.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
34240229	Replication affected post upgrade to 22.2.0 when TLS is used for Georeplication	DBTier Upgrade and Disaster Recovery fails when TLS is used for Georeplication	Upgrade as well as Disaster Recovery fails on TLS enabled cnDBTier georeplication. **Workaround**: Added a step in *Oracle Communications Cloud Native Core DBTier Installation and Upgrade Guide* to upgrade TLS enabled cnDBTier, before starting upgrade of cnDBTier.	3	22.2.0

4.3.3 CNC Console Known Bugs

CNC Console Release 22.2.2

There are no new known bugs in CNC Console Release 22.2.2.

CNC Console Release 22.2.1

There are no new known bugs in CNC Console Release 22.2.1.

CNC Console Release 22.2.0

There are no new known bugs in CNC Console Release 22.2.0.

4.3.4 CNC Policy Known Bugs

CNC Policy 22.2.6 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
34875943	SPAD_POLICY LDAP response metrics are not updated correctly in case failure response from LDAP	The LDAP metrics in case of response failure are being reported twice in count compared to the actual value.	The number of failure response metrics for LDAP call flow will be twice of actual value. **Workaround:** The LDAP failure response alert if configured would need an update to divide the expression calculation by two.	4	22.4.0

The known bugs from CNC Policy Release 22.2.5 are forward ported to Release 22.2.6.

CNC Policy 22.2.5 Known Bugs

There are no new known bugs for this release. The known bugs from CNC Policy Release 22.2.4 are forward ported to Release 22.2.5.

CNC Policy 22.2.4 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
34693710	PCF Upgrade 22.2.3 : Getting PodDisruptionBudget error while upgrading 1.15.5 to 22.2.3-rc7	Failure indicating that the configured/ pre-existing Service Account(s) are not expected when trying to upgrade.	Upgrade Failure **Workaround :** Prior to the upgrade, disable the Service Account, role, and rolebinding manually using the below commands: kubectl delete ServiceAccount <conflict item> -n <namespace> kubectl delete Role <conflict item> -n <namespace> kubectl delete RoleBinding <conflict item> -n <namespace>	3	22.2.0

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
34693684	cnPolicy upgrade fails due to conflict with rolebindings	Upgrade fails as there is conflict with existing rolebindings.	Upgrade failure **Workaround:** If the upgrade for CNC Policy fails due to any of the following conflicts, you are required to delete the conflicting items using the following relevant commands: • In case of conflict due to rolebinding, run the following command: kubectl delete rolebinding -n • In case of conflict due to PodDisruption Budget, run the following command: kubectl delete PodDisruption Budget -n	3	22.2.0

CNC Policy 22.2.3 Known Bugs

There are no known bugs for this release.

CNC Policy 22.2.2 Known Bugs

There are no known bugs for this release.

CNC Policy 22.2.1 Known Bugs

There are no known bugs for this release.

CNC Policy 22.2.0 Known Bugs

Table 4-42 CNC Policy 22.2.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
34224235	ModelD_BindingHeader ATS Feature Failing with EGW 22.2.0	Automated Test Suite do the automated configuration of the feature. In 22.2.0 the configuration is not compatible and Test cases are failing.	Automated test case will not run. There is no impact in the feature as functionality is working properly. **Workaround :** None	3	22.2.0
34224262	MBR Qos values in AAR-I not getting sent in N7 UpdateNotify as MBR/GBR	MBR Qos values in AAR-I is not sent in N7 UpdateNotify as MBR/GBR.		3	22.1.0
34224296	ATS regression failure in initial run	There are intermittent failure for 2 test cases and passing in Second Run. These are warm up issues and after initial run the test cases will pass.	In initial run of ATS test case may fail but it will pass in subsequent runs. **Workaround :** None	3	22.2.0
34225919	SBI Rate Limit is not giving the proper rejection code when Error Code Profile is set to 1XX series	SBI Rate Limit is not giving the proper rejection code when Error Code Profile is set to 1XX series.	Not able to select 1XX or 2XX error code. **Workaround**: None	3	22.2.0

Table 4-42 (Cont.) CNC Policy 22.2.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
34225981	Overload Threshold configurations are overwritten during upgrade	On upgrade, several Diameter Overload threshold Configurations are lost in two scenarios.	Customer will lose any threshold configuration added for a service that was not part of the default configuration. They will loose all threshold configuration added after upgrade, if helm has no default configuration for overload threshold. **Workaround:** Take the backup before upgrade and apply the same once upgrade is complete.	3	22.2.0
34226424	pcrf-core applying apnList changes for on-going sessions as well	On addition or deletion of apnList from pcrf-core GUI (settings), configuration changes are applied to new sessions only. There should be no impact on the old sessions.	Any changes done in configuration applies to existing sessions as well. **Workaround**: None	3	22.2.0

Table 4-42 (Cont.) CNC Policy 22.2.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
34226963	usage-mon service is not granting quota when uplinkVolume = 0 even if downlinkVolume & totalVolume is having quota remaining	When any of the uplink or downlink quota is finished and other quota is remaining, for example, when uplink quota limit is exhausted but downlink quota is remaining, usage-mon service sets all the three attribute totalVolume , uplinkVolume and downlinkVolume to 0 and does not grant any quota.	No quota is generated if any one of the uplink, downlink or total volume quota gets exhausted while the others are still available. **Workaround**: None	3	22.2.0
34226980	Default value for Min Volume/Time Grant & Max Volume/Time Grant are same in Usage Monitoring screen	Min Volume/ Time Grant and Max Volume/Time Grant values in Usage Monitoring screen are same in GUI because of that PCRF grants only that values in GUI as every time either Max or Min Grant values are only matching. Min and Max Grant values should be different.	Same Granted Service Unit is provided. **Workaround**: Set Min Grant lower than Max Grant in GUI.	3	22.2.0

Table 4-42 (Cont.) CNC Policy 22.2.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
34227033	UDR_UMDATA_COMPARE_FLAG not working on PDS	UDR_UMDATA_COMPARE_FLAG is not working in PDS.	PGW receives RAR (depends on Policy) on every UDR notification if smPolicySnssaiData changes in on-going session. **Workaround:** None	3	22.2.0

4.3.5 CNE Known Bugs

CNE Release 22.2.3

There are no new known bugs in this release.

CNE Release 22.2.2

There are no new known bugs in this release.

CNE Release 22.2.1

There are no new known bugs in this release.

CNE Release 22.2.0

Table 4-43 CNE 22.2.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
34218372	vCNE 22.2.0 on VMware validation is incomplete	OCCNE 22.2.0 is released without completion of full validation of vCNE on VMware.	It is recommended to not upgrade vCNE 22.2.0 on VMware until further notice. **Workaround**: None	3	22.2.0

4.3.6 NEF Known Bugs

OCNEF Release 22.2.2

There are no known bugs.

OCNEF Release 22.2.1

There are no known bugs.

OCNEF Release 22.2.0

There are no known bugs.

4.3.7 NRF Known Bugs

OCNRF Release 22.2.3

There are no new known bugs in this release. For existing known bugs, see OCNRF Release 22.2.0.

OCNRF Release 22.2.2

Table 4-44 NRF 22.2.2 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
34882403	NRF Upgrade to 22.2.2 caused Replication Channel down alert	After DBTier upgrade of NRF 22.2.2 to 22.3.0, DB replication is lost.	System outage. **Workaround**: “replication-resync” can be performed to bring back the replication.	1	22.2.0

For existing known bugs, see OCNRF Release 22.2.0.

OCNRF Release 22.2.1

There are no new known bugs in this release. For existing known bugs, see OCNRF Release 22.2.0.

OCNRF Release 22.2.0

Table 4-45 NRF 22.2.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
34205881	DNS NAPTR: DNS record can be stale if deregister request of AMF is not successfully processed by OCNRF	DNS NAPTR: 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.	While processing deregister or suspended requests, if some software fault or network fault occurs, there can be stale records in DNS server. **Workaround**: Stale NAPTR records need to be deleted at DNS Server.	4	22.2.0

Table 4-45   (Cont.) NRF 22.2.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
34205878	DNS NAPTR: Change of AMFName, AMFRegionId, AMF SetId can result into inconsistent data in DNS Server	Change of AMFName, AMFRegionId, AMF SetId can result in inconsistent data in DNS Server. In DNS server, Lookup domain name record may exist without any Replacement record and vice-versa.	In Production, AMFName, AMFRegionId, AMF SetId values are set as per deployment planning as these are AMF identifiers. **Workaround**: 3GPP Attributes AMFName and AMFRegionId/AMF SetId are updated in single request during 3GPP NFUpdate or NFRegister service operations. This will make sure that AMFSetFqdn and replacement values generated by above attributes are different from previous values, hence there are not inconsistent data.	4	22.2.0

Table 4-45 (Cont.) NRF 22.2.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
34205871	3gpp-Sbi-Correlation-Info header not populated in response generated from Ingress Gateway and NRF microservices framework	3gpp-Sbi-Correlation-Info header is not populated in response generated from Ingress Gateway and NRF microservices framework.	This issue is observed in overload cases. **Workaround**: No Workaround available.	4	22.2.0
34205693	DNS NAPTR: Complete removal of ipv4EndpointAddress or ipv6EndpointAddress in n2InterfaceAmfInfo is not resulting into removal from DNS Server	Complete removal of ipv4EndpointAddress or ipv6EndpointAddress inn2InterfaceAmfInfo is not resulting in removal from DNS Server. Issue: NFUPDATE service operation to remove ipv4EndpointAddress complete attribute or ipv6EndpointAddress complete attribute in n2InterfaceAmfInfoAAAA, A NAPTR Records are not removed.	It can occur when operator wants to remove complete list of Ipv4 and Ipv6. Then it is not getting removed from DNS server. **Workaround**: Addition of new IPAddress in ipv4EndpointAddress using NFUpdate can be done. Afterwards, old IPAddress can be removed using same service operation. This is applicable to ipv6EndpointAddress too.	4	22.2.0

Table 4-45 (Cont.) NRF 22.2.0 Known Bugs

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

4.3.8 NSSF Known Bugs

NSSF 22.2.2 Known Bugs

There are no new known bugs in this release.

NSSF 22.2.1 Known Bugs

There are no new known bugs in this release.

NSSF 22.2.0 Known Bugs

Table 4-46 NSSF 22.2.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
34206366	CNCC gui to configure log level is not working for APP logs	NSSF has introduced both application level logs and package level logs in the support for CNC Console. The application level logs are for the logs of the application and package level logs are for the logs generated by the jar. Due to this bug, the application level log can not be configured using CNC Console.	The application level logs cannot be configured using CNC Console. **Workaround**: The application level logs and the jars are configured using Package Level Logs configuration in CNC Console.	3	22.2.2

4.3.9 SCP Known Bugs

SCP Release 22.2.4

There are no new known bugs in this release. For existing known bugs, see Table 4-47.

SCP Release 22.2.3

There are no new known bugs in this release. For existing known bugs, see Table 4-47.

SCP Release 22.2.2

There are no new known bugs in this release. For existing known bugs, see Table 4-47.

SCP Release 22.2.1

There are no new known bugs in this release. For existing known bugs, see Table 4-47.

SCP Release 22.2.0

Table 4-47 SCP 22.2.0 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.	4	22.1.0

4.3.10 SEPP Known Bugs

OCSEPP Release 22.2.2

There are no new known bugs in SEPP Release 22.2.2.

OCSEPP Release 22.2.1

There are no new known bugs in SEPP Release 22.2.1.

OCSEPP Release 22.2.0

There are no new known bugs in SEPP Release 22.2.0.

4.3.11 UDR Known Bugs

OCUDR Release 22.2.2

There are no new known bugs in OCUDR Release 22.2.2.

OCUDR Release 22.2.1

Table 4-48 UDR 22.2.1 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
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 UDR-22.2.0, we see that the overloadLevelThreshold value is set to JSON empty array [].	Workaround is provided in upgrade section of*Oracle Communications Cloud Native Core Installation and Upgrade Guide*	3	22.1.0

OCUDR Release 22.2.0

Table 4-49 UDR 22.2.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
34184627	"udr-deploy-performance" deployment not getting removed when UDR uninstalled successfully	"udr-deploy-performance" deployment not getting removed when UDR uninstalled successfully.	This is intermittent issue. Could be a false alarm.	4	22.1.0
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 UDR-22.2.0, we see that the overloadLevelThreshold value is set to JSON empty array [].	Workaround is provided in upgrade section of *Oracle Communications Cloud Native Core Installation and Upgrade Guide*.	3	22.1.0