Oracle® Communications

Cloud Native Core Release Notes

Release 2.22.4
F74396-35
January 2024

Oracle Communications Cloud Native Core Release Notes, Release 2.22.4

F74396-35

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 2.22.4 - F74396-35, January 2024

CNE 22.4.5

Updated the following sections with the details of CNE release 22.4.5:

- Cloud Native Environment (CNE): Updated the feature details for CNE release 22.4.5.
- Media Pack: Updated the media pack details for CNE release 22.4.5.
- Compatibility Matrix: Updated the compatibility matrix information for CNE release 22.4.5.
- CNE Resolved Bugs: Added resolved bugs for CNE release 22.4.5.
- CNE Known Bugs: Added known bugs for CNE release 22.4.5.

Release 2.22.4 - F74396-34, October 2023

Policy 22.4.0

Updated Cloud Native Core Policy (CNC Policy) section with details of the "Subscriber Tracing support for AM and UE Policy" feature.

Release 2.22.4 - F74396-33, October 2023

DBTier 22.4.0, 22.4.1, 22.4.2, 22.4.3, and 22.4.4 Releases

Added bugs for DBTier release 22.4.0, 22.4.1, 22.4.2, 22.4.3, and 22.4.4 in the DBTier Known Bugs section.

Release 2.22.4 - F74396-32, September 2023

DBTier 22.4.4

Updated the following sections with the details of DBTier release 22.4.4:

- Media Pack: Updated the media pack details for DBTier release 22.4.4.
- Compatibility Matrix: Updated the compatibility matrix information for DBTier release 22.4.4.
- CNE Resolved Bugs: Added resolved bugs for DBTier release 22.4.4.

CNE 22.4.4

Updated the following sections with the details of CNE release 22.4.4:

- Media Pack: Updated the media pack details for CNE release 22.4.4.
- Compatibility Matrix: Updated the compatibility matrix information for CNE release 22.4.4.
- CNE Resolved Bugs: Added resolved bugs for CNE release 22.4.4.

Release 2.22.4 - F74396-31, September 2023

DBTier 22.4.2 and 22.4.3 Releases

Added bugs for DBTier release 22.4.2 and 22.4.3 in the DBTier Known Bugs section.

Release 2.22.4 - F74396-30, August 2023

SCP 22.4.4 Release
Updated the following sections with the details of SCP release 22.4.4:

- Media Pack: Updated the media pack details for SCP release 22.4.4.
- Compatibility Matrix: Updated the compliance matrix information for SCP release 22.4.4.
- Common Microservices Load Lineup: Updated the common services load lineup details for SCP release 22.4.4.
- Security Certification Declaration : Added security declaration for SCP release 22.4.4.
- SCP Resolved Bugs: Added a resolved bug for SCP release 22.4.4.

Release 2.22.4 - F74396-29, August 2023

DBTier 22.4.3 Release
Added a bug in the DBTier Known Bugs section.

Release 2.22.4 - F74396-28, July 2023

Policy 22.4.7 Release
Updated the following sections with the details of Policy release 22.4.7:

- Media Pack: Updated the media pack details for Policy release 22.4.7.
- Compatibility Matrix: Updated the compliance matrix information for Policy release 22.4.7.
- Common Microservices Load Lineup: Updated the common services load lineup details for Policy release 22.4.7.
- Security Certification Declaration : Added security declaration for Policy release 22.4.7.
- CNC Policy Resolved Bugs: Added resolved bugs list for Policy release 22.4.7.

BSF 22.4.7 Release
Updated the following sections with the details of BSF release 22.4.7:

- Media Pack: Updated the media pack details for BSF release 22.4.7.
- Compatibility Matrix: Updated the compliance matrix information for BSF release 22.4.7.
- Common Microservices Load Lineup: Updated the common services load lineup details for BSF release 22.4.7.
- Security Certification Declaration : Added security declaration for BSF release 22.4.7.

Release 2.22.4 - F74396-27, July 2023

CNC Console 22.4.3 Release

Updated the following sections with the details of CNC Console release 22.4.3:

- Media Pack: Updated the media pack details for CNC Console release 22.4.3.

- Compatibility Matrix: Updated the compatibility matrix information for CNC Console release 22.4.3.
- Common Microservices Load Lineup: Updated the common services load lineup details for CNC Console release 22.4.3.
- Security Certification Declaration : Added security declaration for CNC Console release 22.4.3.

NEF 22.4.4 Release

Updated the following sections with the details of NEF release 22.4.4:

- Media Pack: Updated the media pack details for NEF release 22.4.4.
- Compatibility Matrix: Updated the compatibility matrix information for NEF release 22.4.4.
- Common Microservices Load Lineup: Updated the common services load lineup details for NEF release 22.4.4.
- Security Certification Declaration : Added security declaration for NEF release 22.4.4.

SEPP 22.4.4 Release

Updated the following sections with the details of SEPP release 22.4.4:

- Media Pack: Updated the media pack details for SEPP release 22.4.4.
- Compatibility Matrix: Updated the compatibility matrix information for SEPP release 22.4.4.
- Common Microservices Load Lineup: Updated the common services load lineup details for SEPP release 22.4.4.
- Security Certification Declaration : Added security declaration for SEPP release 22.4.4.

Release 2.22.4 - F74396-26, July 2023

NRF 22.4.4 Release

Updated the following sections with the details of NRF release 22.4.4:

- Media Pack: Updated the media pack details for NRF release 22.4.4.
- Compatibility Matrix: Updated the compatibility matrix information for NRF release 22.4.4.
- Common Microservices Load Lineup: Updated the common services load lineup details for NRF release 22.4.4.
- Security Certification Declaration : Added security declaration for NRF release 22.4.4.
- NRF Resolved Bugs: Added resolved bugs for NRF release 22.4.4.
- NRF Known Bugs: Added known bugs for NRF release 22.4.4.

Release 2.22.4 - F74396-25, July 2023

DBTier 22.4.3 Release

Added a new bug in the DBTier Resolved Bugs section.

Release 2.22.4 - F74396-24, July 2023

DBTier 22.4.3 Release

Updated the following sections with the details of DBTier release 22.4.3:

- Media Pack: Updated the media pack details for DBTier release 22.4.3.
- Compatibility Matrix: Updated the compatibility matrix information for DBTier release 22.4.3.
- DBTier Resolved Bugs: Added resolved bugs for DBTier release 22.4.3.

Release 2.22.4 - F74396-23, June 2023

Policy 22.4.6 Release
Updated the following sections with the details of Policy release 22.4.6:

- Media Pack: Updated the media pack details for Policy release 22.4.6.
- Compatibility Matrix: Updated the compliance matrix information for Policy release 22.4.6.
- Common Microservices Load Lineup: Updated the common services load lineup details for Policy release 22.4.6.
- Security Certification Declaration : Added security declaration for Policy release 22.4.6.
- CNC Policy Resolved Bugs: Added resolved bugs list for Policy release 22.4.6.

Release 2.22.4 - F74396-22, May 2023

Policy 22.4.5 Release

- CNC Policy Resolved Bugs: Updated the title for the resolved bug 35158666.

CNC Console 22.4.2 Release

- CNC Console Resolved Bugs: Updated the title for the resolved bug 35154799.

Release 2.22.4 - F74396-21, April 2023

CNE 22.4.3 Release
Updated the following sections with the details of CNE release 22.4.3:

- Cloud Native Environment (CNE): Updated the feature details for CNE release 22.4.3.
- Media Pack: Updated the media pack details for CNE release 22.4.3.
- Compatibility Matrix: Updated the compatibility matrix information for CNE release 22.4.3.
- CNE Resolved Bugs: Added resolved bugs for CNE release 22.4.3.
- CNE Known Bugs: Added known bugs for CNE release 22.4.3.

CNE 22.4.2 Release
Cloud Native Environment (CNE): Added upgrade considerations for CNE release 22.4.2.

Release 2.22.4 - F74396-20, April 2023

CDCS 22.4.2 Release
Updated the following sections with the details of CDCS release 22.4.2:

- Continuous Delivery Control Server (CDCS): Added the feature details for CDCS release 22.4.2.
- Media Pack: Updated the media pack details for CDCS release 22.4.2.

- Compatibility Matrix: Updated the compliance matrix information for CDCS release 22.4.2.
- CDCS Resolved Bugs: Added resolved bugs list for CDCS release 22.4.2.

Release 2.22.4 - F74396-19, April 2023

CNC Console 22.4.2 Release

Updated the following sections with the details of CNC Console release 22.4.2:

- Media Pack: Updated the media pack details for CNC Console release 22.4.2.
- Compatibility Matrix: Updated the compatibility matrix information for CNC Console release 22.4.2.
- Common Microservices Load Lineup: Updated the common services load lineup details for CNC Console release 22.4.2.
- Security Certification Declaration : Added security declaration for CNC Console release 22.4.2.
- CNC Console Resolved Bugs: Added resolved bugs for CNC Console release 22.4.2.

CNE 22.4.2 Release

Updated the following sections with the details of CNE release 22.4.2:

- Cloud Native Environment (CNE): Updated the feature details for CNE release 22.4.2.
- Media Pack: Updated the media pack details for CNE release 22.4.2.
- Compatibility Matrix: Updated the compatibility matrix information for CNE release 22.4.2.
- CNE Resolved Bugs: Added resolved bugs for CNE release 22.4.2.
- CNE Known Bugs: Added known bugs for CNE release 22.4.2.

DBTier 22.4.2 Release

Updated the following sections with the details of DBTier release 22.4.2:

- Media Pack: Updated the media pack details for DBTier release 22.4.2.
- Compatibility Matrix: Updated the compatibility matrix information for DBTier release 22.4.2.
- DBTier Resolved Bugs: Added resolved bugs for DBTier release 22.4.2.

NEF 22.4.3 Release

Updated the following sections with the details of NEF release 22.4.3:

- Media Pack: Updated the media pack details for NEF release 22.4.3.
- Compatibility Matrix: Updated the compatibility matrix information for NEF release 22.4.3.
- Common Microservices Load Lineup: Updated the common services load lineup details for NEF release 22.4.3.
- Security Certification Declaration : Added security declaration for NEF release 22.4.3.
- NEF Resolved Bugs: Added resolved bugs for NEF release 22.4.3.

NSSF 22.4.4 Release

Updated the following sections with the details of NSSF release 22.4.4:

- Media Pack: Updated the media pack details for NSSF release 22.4.4.
- Compatibility Matrix: Updated the compatibility matrix information for NSSF release 22.4.4.
- Common Microservices Load Lineup: Updated the common services load lineup details for NSSF release 22.4.4.
- Security Certification Declaration : Added security declaration for NSSF release 22.4.4.
- NSSF Resolved Bugs: Added resolved bugs for NSSF release 22.4.4.
- NSSF Known Bugs: Added known bugs for NSSF release 22.4.4.

SCP 22.4.3 Release

Updated the following sections with the details of SCP release 22.4.3:

- Media Pack: Updated the media pack details for SCP release 22.4.3.
- Compatibility Matrix: Updated the compliance matrix information for SCP release 22.4.3.
- Common Microservices Load Lineup: Updated the common services load lineup details for SCP release 22.4.3.
- Security Certification Declaration : Added security declaration for SCP release 22.4.3.
- SCP Resolved Bugs: Added resolved bugs list for SCP release 22.4.3.

SEPP 22.4.3 Release

Updated the following sections with the details of SEPP release 22.4.3:

- Media Pack: Updated the media pack details for SEPP release 22.4.3.
- Compatibility Matrix: Updated the compatibility matrix information for SEPP release 22.4.3.
- Common Microservices Load Lineup: Updated the common services load lineup details for SEPP release 22.4.3.
- Security Certification Declaration : Added security declaration for SEPP release 22.4.3.
- SEPP Resolved Bugs: Added resolved bugs for SEPP release 22.4.3.
- SEPP Known Bugs: Added known bugs for SEPP release 22.4.3.

UDR 22.4.2 Release

Updated the following sections with the details of UDR release 22.4.2:

- Media Pack: Updated the media pack details for UDR release 22.4.2.
- Compatibility Matrix: Updated the compatibility matrix information for UDR release 22.4.2.
- Common Microservices Load Lineup: Updated the common services load lineup details for UDR release 22.4.2.
- Security Certification Declaration : Added security declaration for UDR release 22.4.2.
- UDR Resolved Bugs: Added resolved bugs for UDR release 22.4.2.

Release 2.22.4 - F74396-18, April 2023

BSF 22.4.5 Release

Updated the following sections with the details of BSF release 22.4.5:

- Media Pack: Updated the media pack details for BSF release 22.4.5.
- Compatibility Matrix: Updated the compliance matrix information for BSF release 22.4.5.
- Common Microservices Load Lineup: Updated the common services load lineup details for BSF release 22.4.5.
- Security Certification Declaration : Added security declaration for BSF release 22.4.5.
- BSF Resolved Bugs: Added resolved bugs list for BSF release 22.4.5.
- BSF Known Bugs: Added known bugs list for BSF release 22.4.5.

Policy 22.4.5 Release

Updated the following sections with the details of Policy release 22.4.5:

- Media Pack: Updated the media pack details for Policy release 22.4.5.
- Compatibility Matrix: Updated the compliance matrix information for Policy release 22.4.5.
- Common Microservices Load Lineup: Updated the common services load lineup details for Policy release 22.4.5.
- Security Certification Declaration : Added security declaration for Policy release 22.4.5.
- CNC Policy Resolved Bugs: Added resolved bugs list for Policy release 22.4.5.
- CNC Policy Known Bugs: Added known bugs list for Policy release 22.4.5.

Release 2.22.4 - F74396-17, April 2023

NRF 22.4.3 Release

Updated the following sections with the details of NRF release 22.4.3:

- Media Pack: Updated the media pack details for NRF release 22.4.3.
- Compatibility Matrix: Updated the compliance matrix information for NRF release 22.4.3.
- Common Microservices Load Lineup: Updated the common services load lineup details for NRF release 22.4.3.
- Security Certification Declaration : Added security declaration for NRF release 22.4.3.
- NRF Resolved Bugs: Added resolved bugs list for NRF release 22.4.3.
- NRF Known Bugs: Added known bugs list for NRF release 22.4.3.

Release 2.22.4 - F74396-16, March 2023

NRF 22.4.2 Release

Updated the following sections with the details of NRF release 22.4.2:

- Network Repository Function (NRF): Added the feature details for NRF release 22.4.2.
- Media Pack: Updated the media pack details for NRF release 22.4.2.
- Compatibility Matrix: Updated the compliance matrix information for NRF release 22.4.2.

- Common Microservices Load Lineup: Updated the common services load lineup details for NRF release 22.4.2.
- Security Certification Declaration : Added security declaration for NRF release 22.4.2.
- NRF Resolved Bugs: Added resolved bugs list for NRF release 22.4.2.
- NRF Known Bugs: Added known bugs list for NRF release 22.4.2.

Release 2.22.4 - F74396-15, February 2023

SEPP 22.4.2 Release

Updated the following sections with the details of SEPP release 22.4.2:

- Media Pack: Updated the media pack details for SEPP release 22.4.2.
- Compatibility Matrix: Updated the compliance matrix information for SEPP release 22.4.2.
- Common Microservices Load Lineup: Updated the common services load lineup details for SEPP release 22.4.2.
- Security Certification Declaration : Added security declaration for SEPP release 22.4.2.
- SEPP Resolved Bugs: Added resolved bugs list for SEPP release 22.4.2.

Release 2.22.4 - F74396-14, February 2023

CNC Policy 22.4.4 Release

Updated the following sections with the details of CNC Policy release 22.4.4:

- Media Pack: Updated the media pack details for Policy release 22.4.4.
- Compatibility Matrix: Updated the compatibility matrix information for Policy release 22.4.4.
- Common Microservices Load Lineup: Updated the common services load lineup details for Policy release 22.4.4.
- Security Certification Declaration : Added security declaration for Policy release 22.4.4.
- CNC Policy Resolved Bugs: Added a resolved bug for Policy release 22.4.4.
- CNC Policy Known Bugs: Added known bugs list for Policy release 22.4.4.

Release 2.22.4 - F74396-13, February 2023

SCP 22.4.2 Release

Updated the following sections with the details of SCP release 22.4.2:

- Media Pack: Updated the media pack details for SCP release 22.4.2.
- Compatibility Matrix: Updated the compliance matrix information for SCP release 22.4.2.
- Common Microservices Load Lineup: Updated the common services load lineup details for SCP release 22.4.2.
- Security Certification Declaration : Added security declaration for SCP release 22.4.2.

- SCP Resolved Bugs: Added resolved bugs list for SCP release 22.4.2.

NEF 22.4.2 Release

Updated the following sections with the details of NEF release 22.4.2:

- Network Exposure Function (NEF): Added the enhancement details for NEF release 22.4.2.
- Media Pack: Updated the media pack details for NEF release 22.4.2.
- Compatibility Matrix: Updated the compliance matrix information for NEF release 22.4.2.
- Common Microservices Load Lineup: Updated the common services load lineup details for NEF release 22.4.2.
- Security Certification Declaration : Added security declaration for NEF release 22.4.2.
- 'NEF Resolved Bugs: Added a resolved bug for NEF release 22.4.2.

Release 2.22.4 - F74396-12, February 2023

CNC Policy 22.4.3 Release

Updated the following sections with the details of CNC Policy release 22.4.3:

- Media Pack: Updated the media pack details for Policy release 22.4.3.
- Compatibility Matrix: Updated the compatibility matrix information for Policy release 22.4.3.
- Common Microservices Load Lineup: Updated the common services load lineup details for Policy release 22.4.3.
- Security Certification Declaration : Added security declaration for Policy release 22.4.3.
- CNC Policy Resolved Bugs: Added a resolved bug for Policy release 22.4.3.

Release 2.22.4 - F74396-11, February 2023

CNC Policy 22.4.2 Release

Updated the following sections with the details of CNC Policy release 22.4.2:

- Media Pack: Updated the media pack details for Policy release 22.4.2.
- Compatibility Matrix: Updated the compatibility matrix information for Policy release 22.4.2.
- Common Microservices Load Lineup: Updated the common services load lineup details for Policy release 22.4.2.
- Security Certification Declaration : Added security declaration for Policy release 22.4.2.

BSF 22.4.2 Release

Updated the following sections with the details of BSF release 22.4.2:

- Binding Support Function (BSF): Added the feature details for BSF release 22.4.2.
- Media Pack: Updated the media pack details for BSF release 22.4.2.
- Compatibility Matrix: Updated the compliance matrix information for BSF release 22.4.2.
- Common Microservices Load Lineup: Updated the common services load lineup details for BSF release 22.4.2.
- Security Certification Declaration : Added security declaration for BSF release 22.4.2.

Release 2.22.4 - F74396-10, January 2023

CNE 22.4.1 Release
CNE Known Bugs: Added known bugs list for CNE release 22.4.1.

Release 2.22.4 - F74396-09, January 2023

CDCS 22.4.1 Release
Updated the following sections with the details of CDCS release 22.4.1:

- Media Pack: Updated the media pack details for CDCS release 22.4.1.
- Compatibility Matrix: Updated the compliance matrix information for CDCS release 22.4.1.
- CDCS Resolved Bugs: Added resolved bugs list for CDCS release 22.4.1.

Release 2.22.4 - F74396-08, January 2023

CNC Console 22.4.1 Release
Updated the following sections with the details of CNC Console release 22.4.1:

- Media Pack: Updated the media pack details for CNC Console release 22.4.1.
- Compatibility Matrix: Updated the compliance matrix information for CNC Console release 22.4.1.
- Common Microservices Load Lineup: Updated the common services load lineup details for CNC Console release 22.4.1.
- Security Certification Declaration : Added security declaration for CNC Console release 22.4.1.
- CNC Console Resolved Bugs: Added resolved bugs list for CNC Console release 22.4.1.

CNE 22.4.1 Release
Updated the following sections with the details of CNE release 22.4.1:

- Media Pack: Updated the media pack details for CNE release 22.4.1.
- Compatibility Matrix: Updated the compliance matrix information for CNE release 22.4.1.
- CNE Resolved Bugs: Added resolved bugs list for CNE release 22.4.1.

NRF 22.4.1 Release
Updated the following sections with the details of NRF release 22.4.1:

- Media Pack: Updated the media pack details for NRF release 22.4.1.
- Compatibility Matrix: Updated the compliance matrix information for NRF release 22.4.1.
- Common Microservices Load Lineup: Updated the common services load lineup details for NRF release 22.4.1.
- Security Certification Declaration : Added security declaration for NRF release 22.4.1.
- NRF Resolved Bugs: Added resolved bugs list for NRF release 22.4.1.
- NRF Known Bugs: Added known bugs list for NRF release 22.4.1.

UDR 22.4.1 Release

Updated the following sections with the details of UDR release 22.4.1:

- Unified Data Repository (UDR): Added the feature details for UDR release 22.4.1.
- Media Pack: Updated the media pack details for UDR release 22.4.1.
- Compatibility Matrix: Updated the compliance matrix information for UDR release 22.4.1.
- Common Microservices Load Lineup: Updated the common services load lineup details for UDR release 22.4.1.
- Security Certification Declaration : Added security declaration for UDR release 22.4.1.
- UDR Resolved Bugs: Added resolved bugs list for UDR release 22.4.1.

Release 2.22.4 - F74396-07, January 2023

DBTier 22.4.1 Release
Updated the following sections with the details of DBTier release 22.4.1:

- Media Pack: Updated the media pack details for DBTier release 22.4.1.
- Compatibility Matrix: Updated the compliance matrix information for DBTier release 22.4.1.
- DBTier Resolved Bugs: Added resolved bugs list for DBTier release 22.4.1.

NEF 22.4.1 Release
Updated the following sections with the details of NEF release 22.4.1:

- Media Pack: Updated the media pack details for NEF release 22.4.1.
- Compatibility Matrix: Updated the compliance matrix information for NEF release 22.4.1.
- Common Microservices Load Lineup: Updated the common services load lineup details for NEF release 22.4.1.
- Security Certification Declaration : Added security declaration for NEF release 22.4.1.

NSSF 22.4.2 Release
Updated the following sections with the details of NSSF release 22.4.2:

- Media Pack: Updated the media pack details for NSSF release 22.4.2.
- Compatibility Matrix: Updated the compliance matrix information for NSSF release 22.4.2.
- Common Microservices Load Lineup: Updated the common services load lineup details for NSSF release 22.4.2.
- Security Certification Declaration : Added security declaration for NSSF release 22.4.2.
- NSSF Resolved Bugs: Added resolved bugs list for NSSF release 22.4.2.
- NSSF Known Bugs: Added known bugs list for NSSF release 22.4.2.

SCP 22.4.1 Release
Updated the following sections with the details of SCP release 22.4.1:

- Media Pack: Updated the media pack details for SCP release 22.4.1.
- Compatibility Matrix: Updated the compliance matrix information for SCP release 22.4.1.
- Common Microservices Load Lineup: Updated the common services load lineup details for SCP release 22.4.1.
- Security Certification Declaration : Added security declaration for SCP release 22.4.1.
- SCP Resolved Bugs: Added resolved bugs list for SCP release 22.4.1.

SEPP 22.4.1 Release
Updated the following sections with the details of SEPP release 22.4.1:

- Media Pack: Updated the media pack details for SEPP release 22.4.1.
- Compatibility Matrix: Updated the compliance matrix information for SEPP release 22.4.1.
- Common Microservices Load Lineup: Updated the common services load lineup details for SEPP release 22.4.1.
- Security Certification Declaration : Added security declaration for SEPP release 22.4.1
- SEPP Resolved Bugs: Added resolved bugs list for SEPP release 22.4.1.
- SEPP Known Bugs: Added known bugs list for SEPP release 22.4.1.

Release 2.22.4 - F74396-06, January 2023

CNC Policy 22.4.1 Release

Updated the following sections with the details of CNC Policy release 22.4.1:

- Media Pack: Updated the media pack details for Policy release 22.4.1.
- Compatibility Matrix: Updated the compatibility matrix information for Policy release 22.4.1.
- Common Microservices Load Lineup: Updated the common services load lineup details for Policy release 22.4.1.
- Security Certification Declaration : Added security declaration for Policy release 22.4.1.
- CNC Policy Resolved Bugs: Added resolved bugs list for Policy release 22.4.1.
- CNC Policy Known Bugs: Added known bugs list for Policy release 22.4.1.

Release 2.22.4 - F74396-05, December 2022

Changed the name of the 'Compliance Matrix' section to 'Compatibility Matrix'.

NSSF 22.4.1 Release

Updated the following sections with the details of NSSF release 22.4.1:

- Media Pack: Updated the media pack details for NSSF release 22.4.1.
- Compatibility Matrix: Updated the compatibility matrix information for NSSF release 22.4.1.
- Common Microservices Load Lineup: Updated the common services load lineup details for NSSF release 22.4.1.
- Security Certification Declaration : Added security declaration for NSSF release 22.4.1.
- NSSF Resolved Bugs: Added resolved bugs list for NSSF release 22.4.1.

Release 2.22.4 - F74396-04, December 2022

NWDAF 22.1.0 Release
Updated the following sections with the details of NWDAF release 22.1.0:

- Networks Data Analytics Function (NWDAF): Added the feature details for NWDAF release 22.1.0.
- Media Pack: Updated the media pack details for NWDAF release 22.1.0.
- Compatibility Matrix: Updated the compliance matrix information for NWDAF release 22.1.0.
- Common Microservices Load Lineup: Updated the common services load lineup details for NWDAF release 22.1.0.
- Security Certification Declaration : Added security declaration for NWDAF release 22.1.0.

UDR 22.4.0 Release
Updated the following section with the details of UDR release 22.4.0:

- UDR Known Bugs: Added known bugs for UDR release 22.4.0.

Release 2.22.4 - F74396-03, December 2022

DBTier Resolved Bugs: Updated the resolved bug list for DBTier release 22.4.0.

Release 2.22.4 - F74396-02, November 2022

ATS 22.4.0 Release
Updated the following sections with the details of ATS 22.4.0 Release:

- Automated Testing Suite (ATS) Framework: Added the feature details for ATS release 22.4.0.

BSF 22.4.0 Release
Updated the following sections with the details of BSF release 22.4.0:

- Binding Support Function (BSF): Added the feature details for BSF release 22.4.0.
- Media Pack: Updated the media pack details for BSF release 22.4.0.
- Compatibility Matrix: Updated the compliance matrix information for BSF release 22.4.0.
- Common Microservices Load Lineup: Updated the common services load lineup details for BSF release 22.4.0.
- Security Certification Declaration : Added security declaration for BSF release 22.4.0.

CNC Console 22.4.0 Release
Updated the following sections with the details of CNC Console release 22.4.0:

- Cloud Native Core Console (CNC Console): Added the feature details for CNC Console release 22.4.0.
- Media Pack: Updated the media pack details for CNC Console release 22.4.0.
- Compatibility Matrix: Updated the compliance matrix information for CNC Console release 22.4.0.
- Common Microservices Load Lineup: Updated the common services load lineup details for CNC Console release 22.4.0.
- Security Certification Declaration : Added security declaration for CNC Console release 22.4.0.
- CNC Console Resolved Bugs: Added resolved bugs list for CNC Console release 22.4.0.

CNE 22.4.0 Release
Updated the following sections with the details of CNE release 22.4.0:

- Cloud Native Environment (CNE): Added the feature details for CNE release 22.4.0.

- Media Pack: Updated the media pack details for CNE release 22.4.0.
- Compatibility Matrix: Updated the compliance matrix information for CNE release 22.4.0.
- Common Microservices Load Lineup: Updated the common services load lineup details for CNE release 22.4.0.
- Security Certification Declaration : Added security declaration for CNE release 22.4.0.
- CNE Resolved Bugs: Added resolved bugs list for CNE release 22.4.0.

CDCS 22.4.0 Release
Updated the following sections with the details of CDCS release 22.4.0:

- Continuous Delivery Control Server (CDCS): Added the feature details for CDCS release 22.4.0.
- Media Pack: Updated the media pack details for CDCS release 22.4.0.
- Compatibility Matrix: Updated the compliance matrix information for CDCS release 22.4.0.
- CDCS Resolved Bugs: Added resolved bugs list for CDCS release 22.4.0.

DBTier 22.4.0 Release
Updated the following sections with the details of DBTier release 22.4.0:

- Cloud Native Core DBTier (DBTier): Added the feature details for DBTier release 22.4.0.
- Media Pack: Updated the media pack details for DBTier release 22.4.0.
- Compatibility Matrix: Updated the compliance matrix information for DBTier release 22.4.0.
- Common Microservices Load Lineup: Updated the common services load lineup details for DBTier release 22.4.0.
- Security Certification Declaration : Added security declaration for DBTier release 22.4.0.
- DBTier Resolved Bugs: Added resolved bugs list for DBTier release 22.4.0.

NEF 22.4.0 Release
Updated the following sections with the details of NEF release 22.4.0:

- Network Exposure Function (NEF): Added the feature details for NEF release 22.4.0.
- Media Pack: Updated the media pack details for NEF release 22.4.0.
- Compatibility Matrix: Updated the compliance matrix information for NEF release 22.4.0.
- Common Microservices Load Lineup: Updated the common services load lineup details for NEF release 22.4.0.
- Security Certification Declaration : Added security declaration for NEF release 22.4.0.

NRF 22.4.0 Release
Updated the following sections with the details of NRF release 22.4.0:

- Network Repository Function (NRF): Added the feature details for NRF release 22.4.0.

- Media Pack: Updated the media pack details for NRF release 22.4.0.
- Compatibility Matrix: Updated the compliance matrix information for NRF release 22.4.0.
- Common Microservices Load Lineup: Updated the common services load lineup details for NRF release 22.4.0.
- Security Certification Declaration : Added security declaration for NRF release 22.4.0.
- NRF Resolved Bugs: Added resolved bugs list for NRF release 22.4.0.
- NRF Known Bugs: Added known bugs list for NRF release 22.4.0.

NSSF 22.4.0 Release
Updated the following sections with the details of NSSF release 22.4.0:

- Network Slice Selection Function (NSSF): Added the feature details for NSSF release 22.4.0.
- Media Pack: Updated the media pack details for NSSF release 22.4.0.
- Compatibility Matrix: Updated the compliance matrix information for NSSF release 22.4.0.
- Common Microservices Load Lineup: Updated the common services load lineup details for NSSF release 22.4.0.
- Security Certification Declaration : Added security declaration for NSSF release 22.4.0.
- NSSF Resolved Bugs: Added resolved bugs list for NSSF release 22.4.0.
- NSSF Known Bugs: Added known bugs list for NSSF release 22.4.0.

CNC Policy 22.4.0 Release
Updated the following sections with the details of CNC Policy release 22.4.0:

- Cloud Native Core Policy (CNC Policy): Added the feature details for CNC Policy release 22.4.0.
- Media Pack: Updated the media pack details for CNC Policy release 22.4.0.
- Compatibility Matrix: Updated the compliance matrix information for CNC Policy release 22.4.0.
- Common Microservices Load Lineup: Updated the common services load lineup details for CNC Policy release 22.4.0.
- Security Certification Declaration : Added security declaration for CNC Policy release 22.4.0.
- CNC Policy Resolved Bugs: Added resolved bugs list for CNC Policy release 22.4.0.
- CNC Policy Known Bugs: Added known bugs list for CNC Policy release 22.4.0.

SCP 22.4.0 Release
Updated the following sections with the details of SCP release 22.4.0:

- Service Communication Proxy (SCP): Added the feature details for SCP release 22.4.0.
- Media Pack: Updated the media pack details for SCP release 22.4.0.
- Compatibility Matrix: Updated the compliance matrix information for SCP release 22.4.0.
- Common Microservices Load Lineup: Updated the common services load lineup details for SCP release 22.4.0.
- Security Certification Declaration : Added security declaration for SCP release 22.4.0.
- SCP Resolved Bugs: Added resolved bugs list for SCP release 22.4.0.
- SCP Known Bugs: Added known bugs list for SCP release 22.4.0.

SEPP 22.4.0 Release
Updated the following sections with the details of SEPP release 22.4.0:

- Security Edge Protection Proxy (SEPP): Added the feature details for SEPP release 22.4.0.
- Media Pack: Updated the media pack details for SEPP release 22.4.0.
- Compatibility Matrix: Updated the compliance matrix information for SEPP release 22.4.0.
- Common Microservices Load Lineup: Updated the common services load lineup details for SEPP release 22.4.0.
- Security Certification Declaration : Added security declaration for SEPP release 22.4.0.
- SEPP Resolved Bugs: Added resolved bugs list for SEPP release 22.4.0.
- SEPP Known Bugs: Added known bugs list for SEPP release 22.4.0.

UDR 22.4.0 Release
Updated the following sections with the details of UDR release 22.4.0:

- Unified Data Repository (UDR): Added the feature details for UDR release 22.4.0.
- Media Pack: Updated the media pack details for UDR release 22.4.0.
- Compatibility Matrix: Updated the compliance matrix information for UDR release 22.4.0.
- Common Microservices Load Lineup: Updated the common services load lineup details for UDR release 22.4.0.
- Security Certification Declaration : Added security declaration for UDR release 22.4.0.
- UDR Resolved Bugs: Added resolved bugs list for UDR release 22.4.0.
- UDR Known Bugs: Added known bugs list for UDR release 22.4.0.

Common Services Resolved Bugs
Updated the resolved bugs list for the following common services:

- Alternate Route Service Resolved Bugs: Added resolved bugs list for Alternate Route Service.
- App-Info Resolved Bugs: Added resolved bugs list for App-Info.
- Egress Gateway Resolved Bugs: Added resolved bugs list for Egress Gateway.
- Ingress Gateway Resolved Bugs: Added resolved bugs list for Ingress Gateway.
- Mediation Resolved Bugs: Added resolved bug list for Mediation.
- NRF-Client Resolved Bugs: Added resolved bug list for NRF-Client.

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 2.22.4.

2.1 Automated Testing Suite (ATS) Framework

Release 22.4.0

Oracle Communications Cloud Native Core Automated Test Suite (ATS) framework 22.4.0 has been updated with the following enhancement:

- **ATS API**: This feature enables ATS to use the Application Programming Interface (API) to perform regular ATS tasks such as initiating test suites, monitoring test suite execution, and so on. For more information, see "ATS API" in *Oracle Communications Cloud Native Core Automated Testing Suite Guide*.

2.2 Binding Support Function (BSF)

Release 22.4.7

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

Release 22.4.5

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

Release 22.4.2

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

Release 22.4.0

Oracle Communications Cloud Native Core Binding Support Function (BSF) 22.4.0 has been updated with the following enhancements:

- **NF Scoring for a Site**: BSF supports the NF Scoring feature to calculate the site score based on Network Function (NF) specific factors such as metrics, alerts, and so on. The NF Scoring feature helps the operator to determine the health of a site. For more information on this feature and its configurations, see the "NF Scoring for a Site" section in *Oracle Communications Cloud Native Core Binding Support Function User Guide*.
- **Supports Graceful Termination of Kubernetes**: In Kubernetes cluster, pods get deleted due to various events. All applications are notified of the immediate shutdown so that the applications can release all resources in an orderly manner. This feature has been introduced to support the termination of BSF's Kubernetes pods gracefully to reduce traffic loss.

> **Note:**
>
> All features from CNC BSF 22.3.2 are forward ported to 22.4.0.

2.3 Continuous Delivery Control Server (CDCS)

Release 22.4.2

Oracle Communications Cloud Native Core Continuous Delivery Control Server (CDCS) 22.4.2 has been updated with the following enhancements:

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

Release 22.4.1

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

Release 22.4.0

Oracle Communications Cloud Native Core Continuous Delivery Control Server (CDCS) 22.4.0 has been updated with the following enhancements:

- **Support for OCCNE Installation**: CDCS supports OCCNE installation by creating a new Production and Staging Site to install OCCNE. For more information about the installation procedure, see Creating New Production Site and Creating New Staging Site sections in *Oracle Communications CD Control Server User Guide*.
- **Support for Discovering New Software Releases:** : CDCS queries the Oracle FTP Server to determine which new NF releases are available to download by using the Discover New NF Releases on CDCS UI. For more information about the discovering procedure, see Discovering New NF Releases section in *Oracle Communications CD Control Server User Guide*.
- **Performs NF Health Check:** CDCS performs a health check before and after upgrading an NF, and after installing an NF, to ensure that the installation or upgrade was successful. User can perform health check at any time for the NFs. For more information about the verification procedure, see Verifying NF Health section in *Oracle Communications CD Control Server User Guide*.
- **Performs OCCNE Health Check:** CDCS performs a health check before and after upgrading OCCNE, and after installing OCCNE, to ensure that the installation or upgrade was successful. User can perform health check at any time for the OCCNE. For more information about the verification procedure, see Verifying OCCNE Health section in *Oracle Communications CD Control Server User Guide*.
- **NF Dependency Check:** CDCS performs dependency checks between the NF being installed or upgraded and the OCCNE at the target site, and between the NF being installed or upgraded and other NFs that it depends on, before the installation or upgrade is attempted. If any of those dependencies are not satisfied, the installation or upgrade will fail. You can evaluate those dependencies before

attempting the installation or upgrade using the Evaluate Dependencies for NF Release procedure in *Oracle Communications CD Control Server User Guide*.

- **Support to Delete NF Release:** CDCS supports deletion of specific NF release if a user wants to remove a previously downloaded NF release from CDCS to ensure that no one installs that release. The Delete NF Release procedure removes a previously downloaded NF release from the internal CDCS repositories. For more information about the procedure, see Deleting NF Release section in *Oracle Communications CD Control Server User Guide*.
- **Support for Automated CDCS Upgrade:** In the previous release, CDCS provided a manual procedure to upgrade from CDCS release 22.2.x to release 22.3.x. In this release, CDCS supports automated download and upgrade CDCS. For more information about the procedure, Preupgrade Tasks, Upgrade Tasks sections in *Oracle Communications CD Control Server Installation and Upgrade Guide*.
- **Enhancement in Email notification:** Added an option to include the name of the user who initiated each procedure that has been added to the email notification. For more information about the option, see Configuring Email Notification section in *Oracle Communications CD Control Server User Guide*.
- **Option to ignore dependency checks:** A check box has been added to the Install NF and Upgrade NF procedures, when selected, it allows the installation or upgrade to continue even if dependency checks fail. By default, this check box is not selected. You should not check this check box unless the installation or upgrade instructions for the NF you are installing or upgrading instructs you to do so. For more information about the check box, see Installing NF at a Managed Sites and Upgrading NF at a Managed Sites sections in *Oracle Communications CD Control Server User Guide*.
- **Option to automatically rollback if NF upgrade fails:** A check box has been added to the Upgrade NF to auto-rollback the upgrade, if the upgrade fails. For more information about the check box, see Upgrading NF at a Managed Sites section in *Oracle Communications CD Control Server User Guide*.

2.4 Cloud Native Core Console (CNC Console)

Release 22.4.3

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

Release 22.4.2

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

Release 22.4.1

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

Release 22.4.0

Oracle Communications Cloud Native Core Console (CNC Console) 22.4.0 has been updated with the following enhancement:

- **Support for Data Director:** Oracle Communications Data Director (OCDD) is integrated with CNC Console. Features such as authentication, authorization of API/GUI requests, multicluster deployment, multi instance deployment, metrics, alerts, KPIs are supported. For more information, see *Oracle Communications Cloud Native Core Console*

Installation and Upgrade Guide and *Oracle Communications Cloud Native Core Console User Guide*.

- **Support for latest versions of NFs:** CNC Console provides support for existing NFs and Data Director:
  - SCP 22.4.0
  - NRF 22.4.0
  - UDR 22.4.0
  - POLICY 22.4.0
  - BSF 22.4.0
  - SEPP 22.4.0
  - NSSF 22.4.0
  - DD 22.0.0

For more information, see *Oracle Communications Cloud Native Core Console Installation and Upgrade Guide* and *Oracle Communications Cloud Native Core Console User Guide*.

Documentation Enhancements

The CNC Console documentation has been updated with the following enhancements:

- **Document Enhancements in CNC Console Supported Deployment Models:** Console supported deployment models are tested and documented in the Installation Guide. For more information, see *Oracle Communications Cloud Native Core Console Installation and Upgrade Guide*.
- **Document Enhancements to Include cnDBTier Profiles for CNC Console Manager and Agent Deployments:** For each supported Console deployment model corresponding DB Resource Profile and Console resource profile details are documented. For more information, see *Oracle Communications Cloud Native Core Console Installation and Upgrade Guide*.

2.5 Cloud Native Core DBTier (DBTier)

Release 22.4.4

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

Release 22.4.3

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

Release 22.4.2

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

Release 22.4.1

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

Release 22.4.0

Oracle Communications Cloud Native Core DBTier (DBTier) 22.4.0 has been updated with the following enhancements:

- **DBTier Scaling:** DBTier supports horizontal and vertical scaling of MySQL NDB Data PODs which improves the performance of DBTier. For more information about the feature, see "DBTier Scaling" in *Oracle Communications Cloud Native Core DBTier User Guide*.
- **Support for Multichannel Georeplication:** DBTier supports multichannel georeplication feature that improves the georeplication performance between sites by parallelly replicating multiple databases and tables. For more information about the feature, see *Oracle Communications Cloud Native Core DBTier User Guide*.
- **Support for Skip Errors when Active and Standby Replication Channels Disconnect or are Lost:** DBTier supports skipping the cluster disconnect errors. This is done by switching over the replication channel and then skipping the errors by making one of the Replication channel as ACTIVE. The Replication channel with the least epoch value after the cluster disconnect error occurs is selected as ACTIVE. For more information about the feature, see *Oracle Communications Cloud Native Core DBTier User Guide*.
- **Support for Alerts and Metrics to Skip Replication Errors:** DBTier raises alerts if the total number of times the replication errors are skipped is more than the preconfigured values. For more information about the metrics and alerts related to this feature, see "Metrics and Alerts" in *Oracle Communications Cloud Native Core DBTier User Guide*.
- **Support for CNE versions:** DBTier supports the following CNE versions:
  - CNE 22.1.x (K8s 1.21)
  - CNE 22.2.x (K8s 1.22)
  - CNE 22.3.x (K8s 1.23)
  - CNE 22.4.x (K8s 1.23)
- **Support for New Version of MySQL Cluster Software:** The Oracle MySQL Cluster Database software is upgraded to 8.0.31 in this release.

2.6 Cloud Native Environment (CNE)

Release 22.4.5

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

Upgrade Considerations:

- containerd version 1.6.4 is not compatible with Kubernetes version 1.23.7. Therefore, containerd version is downgraded to 1.5.8. If you are upgrading from CNE 22.4.x to 22.4.5 and want to downgrade the containerd version from 1.6.4 to 1.5.8, then perform the following additional steps as part of the standard upgrade procedure:
  1. Before performing an upgrade, add the following line to the active bastion's `occne.ini/hosts.ini` file under the `[occne:vars]` section, to forcefully run the kubespray upgrader:

     ```
     occne_force_k8s_upgrade=True
     ```

2. When the upgrade is complete, remove the following line, that you added in the previous step, from the active bastion's `occne.ini/hosts.ini` file:

   ```
   occne_force_k8s_upgrade=True
   ```

   For more information about the standard upgrade procedure, see *Oracle Communications Cloud Native Environment Upgrade Guide*.

- The `kube_network_node_prefix_value` variable must be defined at the time of installation only. Modifying this variable value during an upgrade leads to upgrade failures. Therefore, retain the same value that is assigned at the time of installation. For information on verifying the `kube_network_node_prefix_value` value, see the "Preupgrade Config Files Check" section of *Oracle Communications Cloud Native Environment Upgrade Guide*.

Release 22.4.4

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

Upgrade Considerations:

- containerd version 1.6.4 is not compatible with Kubernetes version 1.23.7. Therefore, containerd version is downgraded to 1.5.8. If you are upgrading from CNE 22.4.x to 22.4.4 and want to downgrade the containerd version from 1.6.4 to 1.5.8, then perform the following additional steps as part of the standard upgrade procedure:

  1. Before performing an upgrade, add the following line to the active bastion's `occne.ini/hosts.ini` file under the `[occne:vars]` section, to forcefully run the kubespray upgrader:

     ```
     occne_force_k8s_upgrade=True
     ```

  2. When the upgrade is complete, remove the following line, that you added in the previous step, from the active bastion's `occne.ini/hosts.ini` file:

     ```
     occne_force_k8s_upgrade=True
     ```

     For more information about the standard upgrade procedure, see *Oracle Communications Cloud Native Environment Upgrade Guide*.

- The `kube_network_node_prefix_value` variable must be defined at the time of installation only. Modifying this variable value during an upgrade leads to upgrade failures. Therefore, retain the same value that is assigned at the time of installation. For information on verifying the `kube_network_node_prefix_value` value, see the "Preupgrade Config Files Check" section of *Oracle Communications Cloud Native Environment Upgrade Guide*.

Release 22.4.3

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

Upgrade Considerations:

- containerd version 1.6.4 is not compatible with Kubernetes version 1.23.7. Therefore, containerd version is downgraded to 1.5.8. If you are upgrading from CNE 22.4.x to 22.4.3 and want to downgrade the containerd version from 1.6.4 to 1.5.8, then perform the following additional steps as part of the standard upgrade procedure:

  1. Before performing an upgrade, add the following line to the active bastion's `occne.ini/hosts.ini` file under the `[occne:vars]` section, to forcefully run the kubespray upgrader:

     ```
     occne_force_k8s_upgrade=True
     ```

  2. When the upgrade is complete, remove the following line, that you added in the previous step, from the active bastion's `occne.ini/hosts.ini` file:

     ```
     occne_force_k8s_upgrade=True
     ```

     For more information about the standard upgrade procedure, see *Oracle Communications Cloud Native Environment Upgrade Guide*.

- The `kube_network_node_prefix_value` variable must be defined at the time of installation only. Modifying this variable value during an upgrade leads to upgrade failures. Therefore, retain the same value that is assigned at the time of installation. For information on verifying the `kube_network_node_prefix_value` value, see the "Preupgrade Config Files Check" section of *Oracle Communications Cloud Native Environment Upgrade Guide*.

Release 22.4.2

Oracle Communications Cloud Native Core Cloud Native Environment (CNE) 22.4.2 has been updated with the following enhancements:

- **Supports Egress NAT with Multiple Egress Network**: In this release, Egress NAT feature is extended to support Egress network routing. With this enhancement, any pod that performs egress requests can send egress message to multiple networks by providing egress annotations for pods. For more details on configuring this feature, see *Oracle Communications Cloud Native Environment User Guide*.

Upgrade Considerations:
The `kube_network_node_prefix_value` variable must be defined at the time of installation only. Modifying this variable value during an upgrade leads to upgrade failures. Therefore, retain the same variable value that is assigned at the time of installation. For information on verifying the `kube_network_node_prefix_value` value, see the "Preupgrade Config Files Check" section of *Oracle Communications Cloud Native Environment Upgrade Guide*.

Release 22.4.1

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

Release 22.4.0

Oracle Communications Cloud Native Environment (OCCNE) 22.4.0 has been updated with the following enhancements:

- **Network Separation for Egress Requests:** In previous OCCNE releases, all requests generated by an application running on OCCNE contained the source IP of the Kubernetes worker node on which the application pod was running and all Kubernetes

worker nodes got their IP addresses from the same external network. Therefore, all external requests coming from OCCNE had a source IP of that network. This was confusing as the requests arriving at a server outside of OCCNE appeared to be sent from a network other than the one that hosted the server. Also, the security policies in the customer's networking infrastructure blocked these requests. In this release, OCCNE allows an application to select a specific external network and uses an IP address from that network as the source IP field for its egress requests.

- **Private IPs for Kubernetes Worker Nodes:** In previous OCCNE releases, all requests generated by an application running on OCCNE contained the source IP of the Kubernetes worker node on which the application pod was running. This exposed the Kubernetes worker nodes to external access which was a potential security concern. It also required a potentially large number of public IPs to deploy OCCNE. In this release, Kubernetes worker nodes are given IP addresses on the OCCNE internal network. As a result, Kubernetes worker nodes are no longer accessible outside of OCCNE, thereby reducing the attack surface of OCCNE. Also, the number of public IPs required to deploy OCCNE has been significantly reduced.
- **Bastion Host High Availability:** With this release, OCCNE automatically selects an active Bastion Host when the current active Bastion Host fails. Additionally, Bastion Host synchronizes all repositories that includes binary files, container images, Yum packages, and Helm charts. This ensures that when nodes in the Kubernetes cluster need to load container images or Helm charts from the Docker, and Helm repositories hosted on the Bastion Hosts, they get the same images and charts, regardless of which Bastion Host is active.
- **Supports New Version of Common Services:** CNE is compatible with the following common services versions:
  - Helm - 3.8.2
  - Kubernetes - 1.23.7
  - containerd - 1.6.4
  - Calico - 3.22.3
  - MetalLB - 0.12.1
  - Prometheus - 2.36.1
  - Grafana - 7.5.11
  - Jaeger - 1.28.0
  - Istio - 1.14.2 (upgraded)
  - cert-manager - 1.6.2

2.7 Networks Data Analytics Function (NWDAF)

Release 22.1.0

Oracle Communications Networks Data Analytics Function (NWDAF) 22.1.0 has been updated with the following enhancements:

- **NF Load Level Analytics**: A new analytic "NF Load Level" is introduced in Release 22.1.0. With this new feature, the OCNWDAF can provide NF load

analytics information to the analytics consumer. For more information, see *Oracle Communications Network Data Analytics Function User Guide*.

- **Slice Load Level Analytics**: This analytics is updated to include new parameters "Load level information", "Percent UE", "Percent Sessions", and "Number of PDU Sessions". With this enhancement, the slice load level analytics provides more detailed information to the analytics consumer. For more information, see *Oracle Communications Network Data Analytics Function User Guide*.
- **Support for Helm Test**: The OCNWDAF now supports Helm test. Helm Test is a feature that validates the successful installation of OCNWDAF and determines if the NF is ready to take traffic. For more information, see *Oracle Communications Network Data Analytics Function Installation Guide* and *Oracle Communications Network Data Analytics Function Troubleshooting Guide*.
- **Support for OCI Environment:** Starting with release 22.1.0, OCNWDAF can be installed over OCI (Oracle Cloud Infrastructure). For more information about installation, see *Oracle Communications Network Data Analytics Function Installation Guide*.

2.8 Network Exposure Function (NEF)

Release 22.4.4

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

Release 22.4.3

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

Release 22.4.2

Oracle Communications Cloud Native Core Network Exposure Function (NEF) 22.4.2 has been updated with the following enhancement:

- **QoS Session - MediaType:** Starting with release 22.4.2, OCNEF allows `AFSessionWithQOS` procedure to support the `mediaType` parameter in the Policy Control Function (PCF) `Npcf_PolicyAuthorisation` API.

  This parameter is mandatory to have a successful AF Session in QoS procedure with PCF.

Release 22.4.1

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

Release 22.4.0

Oracle Communications Cloud Native Core Network Exposure Function (NEF) 22.4.0 has been updated with the following enhancements:

- **Support for Upgrade**: Starting with release 22.4.0, OCNEF supports the upgrade from the previous releases, such as 22.3.0 and 22.3.1.
- **Support for Rollback**: Starting with release 22.4.0, OCNEF supports the rollback to the previous releases, such as 22.3.0 and 22.3.1.
- **Georedundancy Support**: OCNEF is enhanced to support Geographical Redundant (Georedundant) deployment. It offers two-sites georedundancy to ensure service availability when one of the OCNEF sites is down. For more information, see

"Georedundancy Support" in *Oracle Communications Cloud Native Core Network Exposure Function User Guide*.

2.9 Network Repository Function (NRF)

Release 22.4.4

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

Release 22.4.3

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

Release 22.4.2

Oracle Communications Cloud Native Core Network Repository Functions (NRF) 22.4.2 has been updated with the following enhancements:

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

Release 22.4.1

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

Release 22.4.0

Oracle Communications Cloud Native Core Network Repository Functions (NRF) 22.4.0 has been updated with the following enhancements:

- **Limiting Maximum Allowed Subscriptions**: OCNRF restricts the maximum allowed subscriptions to avoid the overload condition at OCNRF subscription microservice. OCNRF regulates the total number of allowed subscriptions using a configurable Global Subscription Limit. In case of georedundant OCNRFs, the limit is applied across all of the mated sites. For more information, see "Subscription Limit" in *Oracle Communications Cloud Native Core Network Repository Function User Guide*.
- **Message Feed**: OCNRF supports copying of both request and response HTTP messages routed through Ingress and Egress Gateways, to a Data Director. For more information, see "Message Feed" in *Oracle Communications Cloud Native Core Network Repository Function User Guide*.
- **Kubernetes Probe Enhancement in NRF Microservices**: OCNRF supports Startup probe along with enhanced Readiness and Liveliness probes for all the microservices. For more information on the configuration parameters, see *Oracle Communications Cloud Native Core Network Repository Function Installation and Upgrade Guide*.

2.10 Network Slice Selection Function (NSSF)

Release 22.4.4

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

Release 22.4.2

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

Release 22.4.1

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

Release 22.4.0

Oracle Communications Network Slice Selection Function (NSSF) 22.4.0 has been updated with the following enhancements:

- **Support for Overload Control based on Percentage Discards**: The Overload Control feature protects the system from overload and maintains the overall health of OCNSSF. It enables OCNSSF to not only detect the overload conditions but also mitigate such conditions by avoiding entering into an overload situation. For more information, see Overload Control based on Percentage Discards in OCNSSF Supported Features chapter of *Oracle Communications Cloud Native Core Network Slice Selection Function User Guide*.
- **Support for Autopopulation of Configuration Using NRF Content**: Currently, NSSF requires the operator to maintain AMF set data manually in the database, which it uses while responding to initial registration query during the subscription request. This enhancement removes the need for manual configuration by allowing NSSF to autoconfigure AMF information using NRF (Network Repository Function) whenever there is an update in the AMF Set data. For more information, see Autopopulation of Configuration Using NRF Content in OCNSSF Supported Features chapter of *Oracle Communications Cloud Native Core Network Slice Selection Function User Guide*.
- **Support for OAuth Access Token Based Authorization Using Key-ID and NRF Instance ID**: Before this enhancement, NSSF used NRF Instance ID to validate the access token, where Ingress Gateway stored public keys against NRF instance Id. This enhancement allows NSSF to use multiple public certificates for validating Access tokens by adding support for Key-ID (K-ID) based access token validation, in addition to the existing NRF Instance ID based access token validation. For more information, see OAuth Access Token Based Authorization in OCNSSF Supported Features chapter of *Oracle Communications Cloud Native Core Network Slice Selection Function User Guide*.

2.11 Cloud Native Core Policy (CNC Policy)

Release 22.4.7

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

Release 22.4.6

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

Release 22.4.5

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

Release 22.4.4

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

Release 22.4.3

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

Release 22.4.2

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

Release 22.4.1

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

Release 22.4.0

Oracle Communications Cloud Native Core Policy 22.4.0 has been updated with the following enhancements:

- **NF Scoring for a Site**: CNC Policy supports the NF Scoring feature to calculate the site score based on Network Function (NF) specific factors such as metrics, alerts, and so on. The NF Scoring feature helps the operator to determine the health of a site. For more information on this feature and its configurations, see "NF Scoring for a Site" section in *Oracle Communications Cloud Native Core Policy User Guide*.
- **Support for User-Agent Header**: CNC Policy supports the user-agent header, which helps the producer Network Function (NF) to identify the consumer NF that has sent the request. For more information on this feature and its configurations, see "Support for User-Agent Header" section in *Oracle Communications Cloud Native Core Policy User Guide*.
- **Support for Sd interface**: CNC Policy supports the Sd interface that enables it to communicate with the Traffic Detection Function (TDF). In this release, peer nodes sets configuration has been added to set the TDF connection service. For more information on this feature and its configurations, see "Support for Sd Interface" section in *Oracle Communications Cloud Native Core Policy User Guide*.
- **Concurrency Handling for PCRF-Core using Bulwark Service**: PCRF-core supports the Bulwark service to handle the concurrent messages on Gx interface. PCRF-core interacts with Bulwark service using lock and unlock message exchanges by acquiring and releasing the User-IDs based lock upon receiving CCR-I/U/T messages. For more details, see "Support for Concurrency Handling using Bulwark Service in PCRF" section in *Oracle Communications Cloud Native Core Policy User Guide*.
- **Concurrency Handling for SM Service using Bulwark Service**: CNC Policy supports the Bulwark service to handle the concurrent requests coming from other Policy services. The Bulwark service integrates with the SM service to handle the concurrent requests for the SM update-notify procedures. The SM service integration with Bulwark service handles the concurrent requests for the same subscriber in a concurrent and efficient manner. For more details, see "Support for

Concurrency Handling using Bulwark Service" in *Oracle Communications Cloud Native Core Policy User Guide*.

- **Handling Concurrent Notification Requests for PDS Service**: When PDS receives concurrent notification requests for a subscriber (same SUPI) of the same data source, processing multiple notification requests at the same time can result in inaccurate data. To avoid this issue, PDS is integrated with Bulwark Service. Bulwark Service provides lock and unlock mechanism over a SUPI or GPSI key and allows processing of only one notification at a time. For more details, see "Support for Concurrency Handling using Bulwark Service" in Policy section in *Oracle Communications Cloud Native Core Policy User Guide*.
- **Integration with NWDAF**: CNC Policy 22.4.0 includes phase one implementation of CNC Policy integration with NWDAF for testing purposes. This integration helps to get analytics information, which PCF consumes to make policy decisions. For more details, see "NWDAF Agent" section in *Oracle Communications Cloud Native Core Policy User Guide*.
- **Timer Profile in Binding Service**: CNC Policy applies the specific timeout profile while sending request to external NFs. In this release, PCF Binding Service has been updated for BSF. For more details, see "Timer Profiles" section in *Oracle Communications Cloud Native Core Policy User Guide*.
- **Delete Individual URSP Rule For Fragmented Delivery**: CNC Policy is enhanced to support UE service with deletion of URSP rule(s) in subsequent call flows that were previously sent over N1N2 NAS message delivery. For more details, see "UE Policy Enhancements" section in *Oracle Communications Cloud Native Core Policy User Guide*.
- **Support for T3501 Timer Implementation**: CNC Policy supports T3501 Timer for UE policy. For more details, see "PCF UE Policy Service" section in *Oracle Communications Cloud Native Core Policy User Guide*.
- **Database Optimization for the Performance Improvements**: When using a replication setup that involves different sources, it is possible that the same row in a replica is updated by different sources. Conflict resolution in NDB cluster replication resolves such resolution conflicts by providing a user-defined conflict resolution column, which is used to determine whether an update from a source can be applied to the replica or not. Searching the Database for PDSProfile record was time consuming. The PDS search query is optimized by user by selecting the search index in order of preference in CM GUI.
- **Support for Spending Limit Status Reporting**: CNC Policy provides an option to enable spending limit status in each of the create, update, and delete requests from the Policy Services (SM Service, AM Service, and UE Policy Service). The Spending Limit control enables the Policy services to retrieve policy counter status information per subscriber from CHF. That is, by subscribing to spending limit reporting (CHF Data), Policy services can receive notifications on Policy Counters from CHF. For more details, see "Support for Spending Limit Status Reporting" section in *Oracle Communications Cloud Native Core Policy User Guide*.
- **Support for Usage Monitoring in Session Viewer**: CNC Policy now allows viewing the session details for Usage Monitoring service through CNC Console. For more details, see "Session Viewer" section in *Oracle Communications Cloud Native Core Policy User Guide*.
- **Subscriber Tracing support for AM and UE Policy**: CNC Policy is enhanced to support subscriber tracing for AM and UE service. For more details, see "Subscriber Activity Logging" section in *Oracle Communications Cloud Native Core Policy User Guide*.

> **Note:**
>
> All the features from CNC Policy 22.3.1 and 22.3.2 are forward ported to 22.4.0.

2.12 Service Communication Proxy (SCP)

Release 22.4.4

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

Release 22.4.3

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

Release 22.4.2

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

Release 22.4.1

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

Release 22.4.0

Oracle Communications Cloud Native Core Service Communication Proxy (SCP) 22.4.0 has been updated with the following enhancements:

- **Observability Enhancements for SCP Inter-microservice Connectivity**: This enhancement enables SCP to improve the SCP observability by introducing observability parameters to monitor inter-microservices communication failures. For more information, see "Observability Enhancements for SCP Inter-microservice Connectivity" in *Oracle Communications Cloud Native Core Service Communication Proxy User Guide*.
- **Load Control based on the Load Control Information Header**: This feature enables SCP to enhance the existing load control functionality by enabling a direct exchange of the load information between 5G NFs and SCP using the 3gpp-Sbi-Lci header. For more information, see "Load Control based on the Load Control Information Header" in *Oracle Communications Cloud Native Core Service Communication Proxy User Guide*.
- **Message Feed**: The feature allows copying of both request and response messages routed through SCP towards Data Director based on the configuration at SCP. For more information, see "Message Feed" in *Oracle Communications Cloud Native Core Service Communication Proxy User Guide*.
- **Global Egress Rate Limit to Support 75K TPS**: The Global Egress Rate Limit feature is enhanced to support 75000 Transactions Per Second (TPS). For more information, see "Configuring Egress Rate Limiting and Global Egress Rate Limiting" in *Oracle Communications Service Communication Proxy REST Specification Guide*.
- **Outlier Detection Enhancement**: The enhancement enables SCP to track the status of each endpoint of the producer NF or NF services. Upstream producer endpoints that continuously return the service responses with non-2xx status

codes are removed from the routing pool for a predefined period based on the configured non-2xx status codes, counts, and ejection time. For more information, see "Circuit Breaking and Outlier Detection" in *Oracle Communications Cloud Native Core Service Communication Proxy User Guide*.

- **Error Code Generated by SCP**: This is a documentation enhancement to add HTTP error responses generated by SCP. For more information, see "Error Code Generated by SCP" in *Oracle Communications Cloud Native Core Service Communication Proxy User Guide*.
- **Model D Enhancement**: This enhancement introduces the enforceReqSpecificSvcDiscovery parameter to enforce NF Service specific Discovery Request in Model D. For more information, see "Configuring SCP Features" in *Oracle Communications Service Communication Proxy REST Specification Guide*.

2.13 Security Edge Protection Proxy (SEPP)

Release 22.4.4

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

Release 22.4.3

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

Release 22.4.2

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

Release 22.4.1

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

Release 22.4.0

Oracle Communications Cloud Native Core Security Edge Protection Proxy (SEPP) 22.4.0 has been updated with the following enhancements:

- **Hosted SEPP Feature**: Hosted SEPP functionality provides selective routing in Roaming Hub mode.
  - Hosted SEPP can connect to multiple Remote SEPP Sets and allows selective routing between them.
  - Hosted SEPP can not be in the physical network of the partner or can be in the trust boundary of the partner.
  - Global Error Response can be configured on the Hosted SEPP, if routing is not allowed to Remote SEPP Set. For more information about the feature, see the "Hosted SEPP feature" section in *Oracle Communications Cloud Native Core Security Edge Protection Proxy User Guide* and the "Overview" and "Configuration Parameters" sections in *Oracle Communications Cloud Native Core Security Edge Protection Proxy Installation and Upgrade Guide*.
- **Cat 2 - Network ID Validation Feature:** Cat 2 – Network ID Validation feature validates the PLMN ID of P-SEPP in the incoming SBI Request Messages over N32F Interface. This feature allows you to select specific SBI Requests Ingress and Egress to a Remote SEPP Set for which the Network ID Validation will be applied. It is applicable only on SBI request messages and not on SBI responses. For more information about the feature,

see the "CAT-2 Network ID Validation feature" section and the "Configuration Parameters" section in *Oracle Communications Cloud Native Core Security Edge Protection Proxy Installation and Upgrade Guide*.

- **SEPP Message Feed Feature:** This feature allows SEPP to report every incoming and outgoing message onto "Data Director" using the Ingress and Egress Gateways. This would enable SEPP to perform the following activities:
  - Lawful Interception
  - Call Tracing/Tracking
  - Debugging

  Data Director receives the messages from Gateways with a correlation-id and feeds the data securely to an external monitoring system.

  For more information about the feature, see the "SEPP Message Feed Feature" section in *Oracle Communications Cloud Native Core Security Edge Protection Proxy User Guide* and the "Configuration Parameters" section in *Oracle Communications Cloud Native Core Security Edge Protection Proxy Installation and Upgrade Guide*.
- **OSO Integration:** OSO is integrated with SEPP services. OCSEPP supports OSO 22.3.x for common operation services (Prometheus and components such as alertmanager, pushgateway) on a Kubernetes cluster which does not have these common services. For more information on OSO installation procedure, see *Oracle Communications Cloud Native Core Operations Services Overlay Installation Guide*.
- **Supports Integration with Aspen Service Mesh:** SEPP leverages the Platform Service Mesh (for example, Aspen Service Mesh) for all the internal and external TLS communication. The service mesh integration provides inter-NF communication and allows API gateway to co-work with service mesh. The service mesh integration supports the services by deploying a special sidecar proxy in each pod to intercept all network communication between microservices. With this feature, all the SEPP services are leveraged to use ASM.
  For more information on configuring ASM, see "Configuring OCSEPP to support ASM" section in *Oracle Communications Cloud Native Core Security Edge Protection Proxy Installation and Upgrade Guide*.
- **SEPP to Support 30k MPS on a Single Site:** SEPP to support 30k MPS on a single site. For more information on benchmarking details, see *Oracle Communications Cloud Native Core Security Edge Protection Proxy Benchmarking Guide*.
- **Support for Customer Specific CSAR package:** Customer has a specific format to create CSAR package. As a part of this feature, the customer specific CSAR package can be created as per the defined rules.

2.14 Unified Data Repository (UDR)

Release 22.4.2

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

Release 22.4.1

Oracle Communications Cloud Native Core Unified Data Repository (UDR) 22.4.x has been updated with the following enhancements:

- **Equipment Identity Register (EIR) Enhancements**: In this release, EIR supports 14 digit International Mobile Equipment Identity (IMEI). For more information about the feature, see Support for 5G EIR Signaling in *Oracle Communications Cloud Native Core Unified Data Repository User Guide*.

Release 22.4.0

Oracle Communications Cloud Native Core Unified Data Repository (UDR) 22.4.0 has been updated with the following enhancements:

- **Support for Export of Equipment Identity Register (EIR) Subscriber Database**: This feature supports exporting of EIR subscriber database containing all International Mobile Equipment Identity (IMEI) and associated International Mobile Subscriber Identity (IMSI), and Mobile Station Integrated Services Digital Network (MSISDN) using the subscriber export tool. It provides automated and on demand export of the EIR database. For more information about the feature, see Supports Export of SLF and EIR Subscriber Database and Subscriber Export Tool section in *Oracle Communications Cloud Native Core Unified Data Repository User Guide*.
- **Support for Export File Transfer to Remote Server**: In this release, subscriber export tool has been introduced to provide the capability to securely transfer the exported data to a remote server using Secure File Transfer Protocol (SFTP). It also supports monitoring the status of exported data transfer through CNC Console. For more information about the feature, see subscriber export tool section in *Oracle Communications Cloud Native Core Unified Data Repository User Guide*.
- **Support for Remote File Transfer for Bulk Import for EIR**: This feature provides the capability to securely transfer the files from the remote server using SFTP. This feature supports transferring-in the Provisioning Database Interface (PDBI) import files and transferring out the result log files to a remote server. For more information about the feature, see Secure File Transfer Support for Subscriber Bulk Import Tool section in *Oracle Communications Cloud Native Core Unified Data Repository User Guide*.
- **Support for Subscriber Location Function (SLF) - Periodic Export of Subscriber Database**: This feature supports periodic exporting of SLF subscriber data into Comma Separated Value (CSV) file format using the Subscriber Export Tool. The Subscriber Export Tool is scheduled for daily runs and is deployed as a stand-alone tool. It also supports dynamic configuration of periodicity of export. For more information about the feature, see Supports Export of SLF and EIR Subscriber Database and Subscriber Export Tool section in *Oracle Communications Cloud Native Core Unified Data Repository User Guide*.

3
Media and Documentation

3.1 Media Pack

This section lists the media package for Cloud Native Core 2.22.4. 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 2.22.4

Description	NF Version	ATS Package Version	Upgrade Supported
Oracle Communications Cloud Native Core Binding Support Function (BSF)	22.4.7	22.4.7	BSF 22.4.7 supports fresh installation and upgrade from 22.2.x, 22.3.x, and 22.4.x to 22.4.7. 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)	22.4.5	22.4.5	BSF 22.4.5 supports fresh installation and upgrade from 22.3.x, and 22.4.x to 22.4.5. 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)	22.4.2	22.4.1	BSF 22.4.2 supports fresh installation and upgrade from 22.3.x and 22.4.x to 22.4.2. 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 2.22.4

Description	NF Version	ATS Package Version	Upgrade Supported
Oracle Communications Cloud Native Core Binding Support Function (BSF)	22.4.0	22.4.0	BSF 22.4.0 supports fresh installation and upgrade from 22.2.x and 22.3.x to 22.4.0. 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)	22.4.3	NA	CNC Console 22.4.3 supports fresh installation and upgrade from 22.2.x, 22.3.x, and 22.4.x to 22.4.3. For more information, see *Oracle Communications Cloud Native Core Console Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core Console (CNCC)	22.4.2	NA	CNC Console 22.4.2 supports fresh installation and upgrade from 22.2.x and 22.3.x to 22.4.2. For more information, see *Oracle Communications Cloud Native Core Console Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core Console (CNCC)	22.4.1	NA	CNC Console 22.4.1 supports fresh installation and upgrade from 22.2.x and 22.3.x to 22.4.1. For more information, see *Oracle Communications Cloud Native Core Console Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core Console (CNCC)	22.4.0	NA	CNC Console 22.4.0 supports fresh installation and upgrade from 22.2.x and 22.3.x to 22.4.0. For more information, see *Oracle Communications Cloud Native Core Console Installation and Upgrade Guide*.
Oracle Communications Cloud Native Environment (OCCNE)	22.4.5	NA	CNE 22.4.5 supports fresh installation and upgrade from 22.3.x and 22.4.x to 22.4.5. For more information, see *Oracle Communications Cloud Native Environment Installation Guide* and *Oracle Communications Cloud Native Environment Upgrade Guide*.

Table 3-1 (Cont.) Media Pack Contents for Cloud Native Core 2.22.4

Description	NF Version	ATS Package Version	Upgrade Supported
Oracle Communications Cloud Native Environment (OCCNE)	22.4.4	NA	CNE 22.4.4 supports fresh installation and upgrade from 22.3.x and 22.4.x to 22.4.4. For more information, see *Oracle Communications Cloud Native Environment Installation Guide* and *Oracle Communications Cloud Native Environment Upgrade Guide*.
Oracle Communications Cloud Native Environment (OCCNE)	22.4.3	NA	CNE 22.4.3 supports fresh installation and upgrade from 22.3.x and 22.4.x to 22.4.3. For more information, see *Oracle Communications Cloud Native Environment Installation Guide* and *Oracle Communications Cloud Native Environment Upgrade Guide*.
Oracle Communications Cloud Native Environment (OCCNE)	22.4.2	NA	CNE 22.4.2 supports fresh installation and upgrade from 22.3.x and 22.4.x to 22.4.2. For more information, see *Oracle Communications Cloud Native Environment Installation Guide* and *Oracle Communications Cloud Native Environment Upgrade Guide*.
Oracle Communications Cloud Native Environment (OCCNE)	22.4.1	NA	CNE 22.4.1 supports fresh installation and upgrade from 22.3.x to 22.4.1. For more information, see *Oracle Communications Cloud Native Environment Installation Guide* and *Oracle Communications Cloud Native Environment Upgrade Guide*.
Oracle Communications Cloud Native Environment (OCCNE)	22.4.0	NA	CNE 22.4.0 supports fresh installation and upgrade from 22.3.x to 22.4.0. For more information, see *Oracle Communications Cloud Native Environment Installation Guide* and *Oracle Communications Cloud Native Environment Upgrade Guide*.
Oracle Communications Cloud Native Core CD Control Server (CDCS)	22.4.2	NA	CD Control Server 22.4.2 supports fresh installation and upgrade from 22.3.x and 22.4.x to 22.4.2. For more information, see *Oracle Communications CD Control Server Installation and Upgrade Guide*.

Table 3-1 (Cont.) Media Pack Contents for Cloud Native Core 2.22.4

Description	NF Version	ATS Package Version	Upgrade Supported
Oracle Communications Cloud Native Core CD Control Server (CDCS)	22.4.1	NA	CD Control Server 22.4.1 supports fresh installation and upgrade from 22.3.x and 22.4.0 to 22.4.1. For more information, see *Oracle Communications CD Control Server Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core CD Control Server (CDCS)	22.4.0	NA	CD Control Server 22.4.0 supports fresh installation and upgrade from 22.3.x to 22.4.0. For more information, see *Oracle Communications CD Control Server Installation and Upgrade Guide*
Oracle Communications Cloud Native Core DBTier (DBTier)	22.4.4	NA	DBTier 22.4.4 supports fresh installation and upgrade from 22.2.x, 22.3.x, and 22.4.x to 22.4.4. For more information, see *Oracle Communications Cloud Native Core DBTier Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core DBTier (DBTier)	22.4.3	NA	DBTier 22.4.3 supports fresh installation and upgrade from 22.2.x, 22.3.x, and 22.4.x to 22.4.3. For more information, see *Oracle Communications Cloud Native Core DBTier Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core DBTier (DBTier)	22.4.2	NA	DBTier 22.4.2 supports fresh installation and upgrade from 22.2.x, 22.3.x, and 22.4.x to 22.4.2. For more information, see *Oracle Communications Cloud Native Core DBTier Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core DBTier (DBTier)	22.4.1	NA	DBTier 22.4.1 supports fresh installation and upgrade from 22.2.x and 22.3.x to 22.4.1. For more information, see Oracle Communications Cloud Native Core DBTier Installation and Upgrade Guide.
Oracle Communications Cloud Native Core DBTier (DBTier)	22.4.0	NA	DBTier 22.4.0 supports fresh installation and upgrade from 22.2.x and 22.3.x to 22.4.0. For more information, see *Oracle Communications Cloud Native Core DBTier Installation and Upgrade Guide*.

Table 3-1 (Cont.) Media Pack Contents for Cloud Native Core 2.22.4

Description	NF Version	ATS Package Version	Upgrade Supported
Oracle Communications Cloud Native Core Network Exposure Function (NEF)	22.4.4	22.4.4	NEF 22.4.4 supports fresh installation and upgrade only from 22.3.2 and 22.4.x to 22.4.4. For more information on installation, see *Oracle Communications Cloud Native Core Network Exposure Function Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core Network Exposure Function (NEF)	22.4.3	22.4.3	NEF 22.4.3 supports fresh installation and upgrade only from 22.3.2 to 22.4.x. For more information on installation, see *Oracle Communications Cloud Native Core Network Exposure Function Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core Network Exposure Function (NEF)	22.4.2	22.4.2	NEF 22.4.2 supports fresh installation and upgrade only from 22.3.2 to 22.4.x. For more information on installation, see *Oracle Communications Cloud Native Core Network Exposure Function Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core Network Exposure Function (NEF)	22.4.1	22.4.0	NEF 22.4.1 supports fresh installation and upgrade only from 22.3.2 to 22.4.x. For more information on installation, see *Oracle Communications Cloud Native Core Network Exposure Function Installation and Upgrade Guide*. OCNEF does not support upgrade from 22.3.0 or 22.3.1.
Oracle Communications Cloud Native Core Network Exposure Function (NEF)	22.4.0	22.4.0	NEF 22.4.0 supports fresh installation and upgrade from 22.3.x to 22.4.0. For more information on installation, see *Oracle Communications Cloud Native Core Network Exposure Function Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core Network Repository Function (NRF)	22.4.4	22.4.4	NRF 22.4.4 supports fresh installation and upgrade from 22.3.x, 22.4.x to 22.4.4. For more information on installation or upgrading, see *Oracle Communications Cloud Native Core Network Repository Function Installation and Upgrade Guide*.

Table 3-1 (Cont.) Media Pack Contents for Cloud Native Core 2.22.4

Description	NF Version	ATS Package Version	Upgrade Supported
Oracle Communications Cloud Native Core Network Repository Function (NRF)	22.4.3	22.4.3	NRF 22.4.3 supports fresh installation and upgrade from 22.3.x, 22.4.x to 22.4.3. For more information on installation or upgrading, see *Oracle Communications Cloud Native Core Network Repository Function Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core Network Repository Function (NRF)	22.4.2	22.4.2	NRF 22.4.2 supports fresh installation and upgrade from 22.3.x, 22.4.x to 22.4.2. For more information on installation or upgrading, see *Oracle Communications Cloud Native Core Network Repository Function Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core Network Repository Function (NRF)	22.4.1	22.4.1	NRF 22.4.1 supports fresh installation and upgrade from 22.3.x, 22.4.x to 22.4.1. For more information on installation or upgrading, see *Oracle Communications Cloud Native Core Network Repository Function Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core Network Repository Function (NRF)	22.4.0	22.4.0	NRF 22.4.0 supports fresh installation and upgrade from 22.3.x to 22.4.0. For more information on installation or upgrading, see *Oracle Communications Cloud Native Core Network Repository Function Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core Network Slice Selection Function (NSSF)	22.4.4	22.4.4	NSSF 22.4.4 supports fresh installation and upgrade from 22.4.x to 22.4.4. 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)	22.4.2	22.4.2	NSSF 22.4.2 supports fresh installation and upgrade from 22.3.x , 22.4.1 to 22.4.2. For more information on installation, see *Oracle Communications Cloud Native Core Network Slice Selection Function Installation and Upgrade Guide*.

Table 3-1 (Cont.) Media Pack Contents for Cloud Native Core 2.22.4

Description	NF Version	ATS Package Version	Upgrade Supported
Oracle Communications Cloud Native Core Network Slice Selection Function (NSSF)	22.4.1	22.4.1	NSSF 22.4.1 supports fresh installation and upgrade from 22.3.x and 22.4.0 to 22.4.1. For more information on installation, see *Oracle Communications Cloud Native Core Network Slice Selection Function Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core Network Slice Selection Function (NSSF)	22.4.0	22.4.0	NSSF 22.4.0 supports fresh installation and upgrade from 22.3.x to 22.4.0. For more information on installation, see *Oracle Communications Cloud Native Core Network Slice Selection Function Installation and Upgrade Guide*.
Oracle Communications Networks Data Analytics Function (NWDAF)	22.1.0	22.4.0	NWDAF 22.1.0 supports fresh installation only. For more information on installation, see *Oracle Communications Networks Data Analytics Function Installation Guide*.
Oracle Communications Cloud Native Core Policy (CNC Policy)	22.4.7	22.4.7	CNC Policy 22.4.7 supports fresh installation and upgrade from 22.2.x, 22.3.x, and 22.4.x to 22.4.7. 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)	22.4.6	22.4.6	CNC Policy 22.4.6 supports fresh installation and upgrade from 22.3.x and 22.4.x to 22.4.6. 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)	22.4.5	22.4.1	CNC Policy 22.4.5 supports fresh installation and upgrade from 22.3.x and 22.4.x to 22.4.5. 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 2.22.4

Description	NF Version	ATS Package Version	Upgrade Supported
Oracle Communications Cloud Native Core Policy (CNC Policy)	22.4.4	22.4.1	CNC Policy 22.4.4 supports fresh installation and upgrade from 22.3.x and 22.4.x to 22.4.4. 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)	22.4.3	22.4.1	CNC Policy 22.4.3 supports fresh installation and upgrade from 22.3.x and 22.4.x to 22.4.3. 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)	22.4.2	22.4.1	CNC Policy 22.4.2 supports fresh installation and upgrade from 22.3.x and 22.4.x to 22.4.2. 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)	22.4.1	22.4.1	CNC Policy 22.4.1 supports fresh installation and upgrade from 22.3.x and 22.4.x to 22.4.1. 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)	22.4.0	22.4.0	CNC Policy 22.4.0 supports fresh installation and upgrade from 22.2.x and 22.3.x to 22.4.0. 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)	22.4.4	22.4.4	SCP 22.4.4 supports fresh installation and upgrade from 22.2.x, 22.3.x, and 22.4.x to 22.4.4. For more information, see *Oracle Communications Cloud Native Core Service Communication Proxy Installation and Upgrade Guide*.

Table 3-1 (Cont.) Media Pack Contents for Cloud Native Core 2.22.4

Description	NF Version	ATS Package Version	Upgrade Supported
Oracle Communications Cloud Native Core Service Communications Proxy (SCP)	22.4.3	22.4.3	SCP 22.4.3 supports fresh installation and upgrade from 22.2.x, 22.3.x, and 22.4.x to 22.4.3. For more information, see *Oracle Communications Cloud Native Core Service Communication Proxy Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core Service Communications Proxy (SCP)	22.4.2	22.4.2	SCP 22.4.2 supports fresh installation and upgrade from 22.2.x, 22.3.x, and 22.4.x to 22.4.2. For more information, see *Oracle Communications Cloud Native Core Service Communication Proxy Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core Service Communications Proxy (SCP)	22.4.1	22.4.1	SCP 22.4.1 supports fresh installation and upgrade from 22.2.x, 22.3.x, and 22.4.0 to 22.4.1. For more information, see *Oracle Communications Cloud Native Core Service Communication Proxy Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core Service Communications Proxy (SCP)	22.4.0	22.4.0	SCP 22.4.0 supports fresh installation and upgrade from 22.2.x and 22.3.x to 22.4.0. For more information, see *Oracle Communications Cloud Native Core Service Communication Proxy Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core Security Edge Protection Proxy (SEPP)	22.4.4	22.4.4	OCSEPP 22.4.4 supports fresh installation and upgrade from 22.2.x, 22.3.x, 22.4.2, and 22.4.3 to 22.4.4 Roaming Hub mode supports the fresh installation and upgrade from 22.3.x, 22.4.2, and 22.4.3 to 22.4.4. For more information on installation or upgrading, see *Oracle Communications Cloud Native Core Security Edge Protection Proxy Installation and Upgrade Guide*.

Table 3-1 (Cont.) Media Pack Contents for Cloud Native Core 2.22.4

Description	NF Version	ATS Package Version	Upgrade Supported
Oracle Communications Cloud Native Core Security Edge Protection Proxy (SEPP)	22.4.3	22.4.3	SEPP 22.4.3 supports fresh installation and upgrade from 22.2.x, 22.3.x, and 22.4.2 to 22.4.3. Roaming Hub mode supports the fresh installation and upgrade from 22.3.x and 22.4.2 to 22.4.3. 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)	22.4.2	22.4.2	SEPP 22.4.2 supports fresh installation and upgrade from 22.2.x, 22.3.x to 22.4.2. Roaming Hub mode supports the fresh installation and upgrade from 22.3.x to 22.4.2. 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)	22.4.1	22.4.1	SEPP 22.4.1 supports fresh installation and upgrade from 22.2.x, 22.3.x, and 22.4.0 to 22.4.1. Roaming Hub mode supports the fresh installation and upgrade from 22.3.x, 22.4.0 to 22.4.1. 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)	22.4.0	22.4.0	SEPP 22.4.0 supports fresh installation and upgrade from 22.2.x, 22.3.x to 22.4.0. Roaming Hub mode supports the fresh installation and upgrade from 22.3.x to 22.4.0. For more information on installation or upgrading, see *Oracle Communications Cloud Native Core Security Edge Protection Proxy Installation and Upgrade Guide*.

Table 3-1 (Cont.) Media Pack Contents for Cloud Native Core 2.22.4

Description	NF Version	ATS Package Version	Upgrade Supported
Oracle Communications Cloud Native Core Unified Data Repository (UDR)	22.4.2	22.4.2	UDR 22.4.2 supports fresh installation and upgrade from 22.2.x, 22.3.x and 22.4.x to 22.4.2. For more information, see *Oracle Communications Cloud Native Core United Data Repository Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core Unified Data Repository (UDR)	22.4.1	22.4.1	UDR 22.4.1 supports fresh installation and upgrade from 22.2.x, 22.3.x and 22.4.0 to 22.4.1. 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)	22.4.0	22.4.0	UDR 22.4.0 supports fresh installation and upgrade from 22.1.x, 22.2.x, and 22.3.x to 22.4.0. For more information on installation or upgrading, see *Oracle Communications Cloud Native Core United Data Repository Installation and Upgrade Guide*.

3.2 Compatibility Matrix

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

Table 3-2 Compatibility Matrix

CNC NF	NF Version	OCCNE	DBTier	CDCS	OSO	Kubernetes	CNC Console	3GPP
BSF	22.4.7	• 22.4.x • 22.3.x • 22.2.x	• 22.4.x • 22.3.x • 22.2.x	NA	• 22.3.x • 1.10.x • 1.6.x	• 1.23.x • 1.22.x • 1.21.x	22.4.x	• 3GPP TS 23.501 • 3GPP TS 23.502 • 3GPP TS 23.503 • 3GPP TS 29.500 • 3GPP TS 29.504 • 3GPP TS 29.510 • 3GPP TS 29.514 • 3GPP TS 29.521 • 3GPP TS 29.214

Table 3-2 (Cont.) Compatibility Matrix

CNC NF	NF Version	OCCNE	DBTier	CDCS	OSO	Kubernetes	CNC Console	3GPP
BSF	22.4.5	• 22.4.x • 22.3.x • 22.2.x	• 22.4.x • 22.3.x • 22.2.x	NA	• 22.3.x • 1.10.x • 1.6.x	• 1.23.x • 1.22.x • 1.21.x	22.4.x	• 3GPP TS 23.501 • 3GPP TS 23.502 • 3GPP TS 23.503 • 3GPP TS 29.500 • 3GPP TS 29.504 • 3GPP TS 29.510 • 3GPP TS 29.514 • 3GPP TS 29.521 • 3GPP TS 29.214
BSF	22.4.2	• 22.4.x • 22.3.x • 22.2.x	• 22.4.x • 22.3.x • 22.2.x	NA	• 22.3.x • 1.10.x • 1.6.x	• 1.23.x • 1.22.x • 1.21.x	22.4.x	• 3GPP TS 23.501 • 3GPP TS 23.502 • 3GPP TS 23.503 • 3GPP TS 29.500 • 3GPP TS 29.504 • 3GPP TS 29.510 • 3GPP TS 29.514 • 3GPP TS 29.521 • 3GPP TS 29.214
BSF	22.4.0	• 22.4.x • 22.3.x • 22.2.x	• 22.4.x • 22.3.x • 22.2.x	NA	• 22.3.x • 1.10.x • 1.6.x	• 1.23.x • 1.22.x • 1.21.x	22.4.x	• 3GPP TS 23.501 • 3GPP TS 23.502 • 3GPP TS 23.503 • 3GPP TS 29.500 • 3GPP TS 29.504 • 3GPP TS 29.510 • 3GPP TS 29.514 • 3GPP TS 29.521 • 3GPP TS 29.214
CNC Console	22.4.3	• 22.4.x • 22.3.x • 22.2.x	• 22.4.x • 22.3.x • 22.2.x	• 22.4.x • 22.3.x	• 22.3.x • 1.10.x • 1.6.x	• 1.23.x • 1.22.x • 1.21.x	NA	NA
CNC Console	22.4.2	• 22.4.x • 22.3.x • 22.2.x	• 22.4.x • 22.3.x • 22.2.x	• 22.4.x • 22.3.x	• 22.3.x • 1.10.x • 1.6.x	• 1.23.x • 1.22.x • 1.21.x	NA	NA

Table 3-2 (Cont.) Compatibility Matrix

CNC NF	NF Version	OCCNE	DBTier	CDCS	OSO	Kubernetes	CNC Console	3GPP
CNC Console	22.4.1	• 22.4.x • 22.3.x • 22.2.x	• 22.4.x • 22.3.x • 22.2.x	• 22.4.x • 22.3.x	• 22.3.x • 1.10.x • 1.6.x	• 1.23.x • 1.22.x • 1.21.x	NA	NA
CNC Console	22.4.0	• 22.4.x • 22.3.x • 22.2.x	• 22.4.x • 22.3.x • 22.2.x	• 22.4.x • 22.3.x	• 22.3.x • 1.10.x • 1.6.x	• 1.23.x • 1.22.x • 1.21.x	NA	NA
CNC Policy	22.4.7	• 22.4.x • 22.3.x • 22.2.x	• 22.4.x • 22.3.x • 22.2.x	NA	• 22.3.x • 1.10.x • 1.6.x	• 1.23.x • 1.22.x • 1.21.x	22.4.x	• 3GPP TS 23.501 • 3GPP TS 23.502 • 3GPP TS 23.503 • 3GPP TS 29.500 • 3GPP TS 29.504 • 3GPP TS 29.510 • 3GPP TS 29.507 • 3GPP TS 29.512 • 3GPP TS 29.513 • 3GPP TS 29.514 • 3GPP TS 29.519 • 3GPP TS 29.521 • 3GPP TS 29.525 • 3GPP TS 29.594 • 3GPP TS 29.214 • 3GPP TS 29.212
CNC Policy	22.4.6	• 22.4.x • 22.3.x • 22.2.x	• 22.4.x • 22.3.x • 22.2.x	NA	• 22.3.x • 1.10.x • 1.6.x	• 1.23.x • 1.22.x • 1.21.x	22.4.x	• 3GPP TS 23.501 • 3GPP TS 23.502 • 3GPP TS 23.503 • 3GPP TS 29.500 • 3GPP TS 29.504 • 3GPP TS 29.510 • 3GPP TS 29.507 • 3GPP TS 29.512 • 3GPP TS 29.513 • 3GPP TS 29.514 • 3GPP TS 29.519 • 3GPP TS 29.521 • 3GPP TS 29.525 • 3GPP TS 29.594 • 3GPP TS 29.214 • 3GPP TS 29.212

Table 3-2 (Cont.) Compatibility Matrix

CNC NF	NF Version	OCCNE	DBTier	CDCS	OSO	Kubernetes	CNC Console	3GPP
CNC Policy	22.4.5	• 22.4.x • 22.3.x • 22.2.x	• 22.4.x • 22.3.x • 22.2.x	NA	• 22.3.x • 1.10.x • 1.6.x	• 1.23.x • 1.22.x • 1.21.x	22.4.x	• 3GPP TS 23.501 • 3GPP TS 23.502 • 3GPP TS 23.503 • 3GPP TS 29.500 • 3GPP TS 29.504 • 3GPP TS 29.510 • 3GPP TS 29.507 • 3GPP TS 29.512 • 3GPP TS 29.513 • 3GPP TS 29.514 • 3GPP TS 29.519 • 3GPP TS 29.521 • 3GPP TS 29.525 • 3GPP TS 29.594 • 3GPP TS 29.214 • 3GPP TS 29.212
CNC Policy	22.4.4	• 22.4.x • 22.3.x • 22.2.x	• 22.4.x • 22.3.x • 22.2.x	NA	• 22.3.x • 1.10.x • 1.6.x	• 1.23.x • 1.22.x • 1.21.x	22.4.x	• 3GPP TS 23.501 • 3GPP TS 23.502 • 3GPP TS 23.503 • 3GPP TS 29.500 • 3GPP TS 29.504 • 3GPP TS 29.510 • 3GPP TS 29.507 • 3GPP TS 29.512 • 3GPP TS 29.513 • 3GPP TS 29.514 • 3GPP TS 29.519 • 3GPP TS 29.521 • 3GPP TS 29.525 • 3GPP TS 29.594 • 3GPP TS 29.214 • 3GPP TS 29.212

Table 3-2 (Cont.) Compatibility Matrix

CNC NF	NF Version	OCCNE	DBTier	CDCS	OSO	Kubernetes	CNC Console	3GPP
CNC Policy	22.4.3	• 22.4.x • 22.3.x • 22.2.x	• 22.4.x • 22.3.x • 22.2.x	NA	• 22.3.x • 1.10.x • 1.6.x	• 1.23.x • 1.22.x • 1.21.x	22.4.x	• 3GPP TS 23.501 • 3GPP TS 23.502 • 3GPP TS 23.503 • 3GPP TS 29.500 • 3GPP TS 29.504 • 3GPP TS 29.510 • 3GPP TS 29.507 • 3GPP TS 29.512 • 3GPP TS 29.513 • 3GPP TS 29.514 • 3GPP TS 29.519 • 3GPP TS 29.521 • 3GPP TS 29.525 • 3GPP TS 29.594 • 3GPP TS 29.214 • 3GPP TS 29.212
CNC Policy	22.4.2	• 22.4.x • 22.3.x • 22.2.x	• 22.4.x • 22.3.x • 22.2.x	NA	• 22.3.x • 1.10.x • 1.6.x	• 1.23.x • 1.22.x • 1.21.x	22.4.x	• 3GPP TS 23.501 • 3GPP TS 23.502 • 3GPP TS 23.503 • 3GPP TS 29.500 • 3GPP TS 29.504 • 3GPP TS 29.510 • 3GPP TS 29.507 • 3GPP TS 29.512 • 3GPP TS 29.513 • 3GPP TS 29.514 • 3GPP TS 29.519 • 3GPP TS 29.521 • 3GPP TS 29.525 • 3GPP TS 29.594 • 3GPP TS 29.214 • 3GPP TS 29.212

Table 3-2 (Cont.) Compatibility Matrix

CNC NF	NF Version	OCCNE	DBTier	CDCS	OSO	Kubernetes	CNC Console	3GPP
CNC Policy	22.4.1	• 22.4.x • 22.3.x • 22.2.x	• 22.4.x • 22.3.x • 22.2.x	NA	• 22.3.x • 1.10.x • 1.6.x	• 1.23.x • 1.22.x • 1.21.x	22.4.x	• 3GPP TS 23.501 • 3GPP TS 23.502 • 3GPP TS 23.503 • 3GPP TS 29.500 • 3GPP TS 29.504 • 3GPP TS 29.510 • 3GPP TS 29.507 • 3GPP TS 29.512 • 3GPP TS 29.513 • 3GPP TS 29.514 • 3GPP TS 29.519 • 3GPP TS 29.521 • 3GPP TS 29.525 • 3GPP TS 29.594 • 3GPP TS 29.214 • 3GPP TS 29.212
CNC Policy	22.4.0	• 22.4.x • 22.3.x • 22.2.x	• 22.4.x • 22.3.x • 22.2.x	NA	• 22.3.x • 1.10.x • 1.6.x	• 1.23.x • 1.22.x • 1.21.x	22.4.x	• 3GPP TS 23.501 • 3GPP TS 23.502 • 3GPP TS 23.503 • 3GPP TS 29.500 • 3GPP TS 29.504 • 3GPP TS 29.510 • 3GPP TS 29.507 • 3GPP TS 29.512 • 3GPP TS 29.513 • 3GPP TS 29.514 • 3GPP TS 29.519 • 3GPP TS 29.521 • 3GPP TS 29.525 • 3GPP TS 29.594 • 3GPP TS 29.214 • 3GPP TS 29.212
CNE	22.4.5	NA	NA	NA	NA	1.23.x	NA	NA
CNE	22.4.4	NA	NA	NA	NA	1.23.x	NA	NA
CNE	22.4.3	NA	NA	NA	NA	1.23.x	NA	NA
CNE	22.4.2	NA	NA	NA	NA	1.23.x	NA	NA
CNE	22.4.1	NA	NA	NA	NA	1.23.x	NA	NA
CNE	22.4.0	NA	NA	NA	NA	1.23.x	NA	NA
CDCS	22.4.2	22.4.x	22.4.x	NA	NA	• 1.23.x • 1.22.x	NA	NA
CDCS	22.4.1	22.4.x	22.4.x	NA	NA	• 1.23.x • 1.22.x	NA	NA
CDCS	22.4.0	22.4.x	22.4.x	NA	NA	• 1.23.x • 1.22.x	NA	NA

Table 3-2 (Cont.) Compatibility Matrix

CNC NF	NF Version	OCCNE	DBTier	CDCS	OSO	Kubernetes	CNC Console	3GPP
DBTier	22.4.4	• 22.4.x • 22.3.x • 22.2.x • 22.1.x	NA	22.4.x	NA	• 1.23.x • 1.22.x • 1.21.x	NA	NA
DBTier	22.4.3	• 22.4.x • 22.3.x • 22.2.x • 22.1.x	NA	22.4.x	NA	• 1.23.x • 1.22.x • 1.21.x	NA	NA
DBTier	22.4.2	• 22.4.x • 22.3.x • 22.2.x • 22.1.x	NA	22.4.x	NA	• 1.23.x • 1.22.x • 1.21.x	NA	NA
DBTier	22.4.1	• 22.4.x • 22.3.x • 22.2.x • 22.1.x	NA	22.4.x	NA	• 1.23.x • 1.22.x • 1.21.x	NA	NA
DBTier	22.4.0	• 22.4.x • 22.3.x • 22.2.x • 22.1.x	NA	22.4.x	NA	• 1.23.x • 1.22.x • 1.21.x	NA	NA
NEF	22.4.4	• 22.3.x • 22.2.x • 22.1.x	• 22.3.x • 22.2.x • 22.1.x	NA	NA	• 1.23.x • 1.22.x • 1.21.x	NA	• 3GPP TS 23.222 v16.9.0 • 3GPP TS 23.501 v16.7.0 • 3GPP TS 23.502 v16.7.0 • 3GPP TS 29.122 v16.8.0 • 3GPP TS 29.222 v16.5.0 • 3GPP 29.500 v16.6.0 • 3GPP 29.501 v16.6.0 • 3GPP TS 29.522 v16.6.0 • 3GPP 29.510 v16.6.0 • 3GPP TS 29.591 v16.3.0

Table 3-2 (Cont.) Compatibility Matrix

CNC NF	NF Version	OCCNE	DBTier	CDCS	OSO	Kubernetes	CNC Console	3GPP
NEF	22.4.3	• 22.3.x • 22.2.x • 22.1.x	• 22.3.x • 22.2.x • 22.1.x	NA	NA	• 1.23.x • 1.22.x • 1.21.x	NA	• 3GPP TS 23.222 v16.9.0 • 3GPP TS 23.501 v16.7.0 • 3GPP TS 23.502 v16.7.0 • 3GPP TS 29.122 v16.8.0 • 3GPP TS 29.222 v16.5.0 • 3GPP 29.500 v16.6.0 • 3GPP 29.501 v16.6.0 • 3GPP TS 29.522 v16.6.0 • 3GPP 29.510 v16.6.0 • 3GPP TS 29.591 v16.3.0
NEF	22.4.2	• 22.3.x • 22.2.x • 22.1.x	• 22.3.x • 22.2.x • 22.1.x	NA	NA	• 1.23.x • 1.22.x • 1.21.x	NA	• 3GPP TS 23.222 v16.9.0 • 3GPP TS 23.501 v16.7.0 • 3GPP TS 23.502 v16.7.0 • 3GPP TS 29.122 v16.8.0 • 3GPP TS 29.222 v16.5.0 • 3GPP 29.500 v16.6.0 • 3GPP 29.501 v16.6.0 • 3GPP TS 29.522 v16.6.0 • 3GPP 29.510 v16.6.0 • 3GPP TS 29.591 v16.3.0

Table 3-2 (Cont.) Compatibility Matrix

CNC NF	NF Version	OCCNE	DBTier	CDCS	OSO	Kubernetes	CNC Console	3GPP
NEF	22.4.1	• 22.3.x • 22.2.x • 22.1.x	• 22.3.x • 22.2.x • 22.1.x	NA	NA	• 1.23.x • 1.22.x • 1.21.x	NA	• 3GPP TS 23.222 v16.9.0 • 3GPP TS 23.501 v16.7.0 • 3GPP TS 23.502 v16.7.0 • 3GPP TS 29.122 v16.8.0 • 3GPP TS 29.222 v16.5.0 • 3GPP 29.500 v16.6.0 • 3GPP 29.501 v16.6.0 • 3GPP TS 29.522 v16.6.0 • 3GPP 29.510 v16.6.0 • 3GPP TS 29.591 v16.3.0
NEF	22.4.0	• 22.3.x • 22.2.x • 22.1.x	• 22.3.x • 22.2.x • 22.1.x	NA	NA	• 1.23.x • 1.22.x • 1.21.x	NA	• 3GPP TS 23.222 v16.9.0 • 3GPP TS 23.501 v16.7.0 • 3GPP TS 23.502 v16.7.0 • 3GPP TS 29.122 v16.8.0 • 3GPP TS 29.222 v16.5.0 • 3GPP 29.500 v16.6.0 • 3GPP 29.501 v16.6.0 • 3GPP TS 29.522 v16.6.0 • 3GPP 29.510 v16.6.0 • 3GPP TS 29.591 v16.3.0
NRF	22.4.4	• 22.4.x • 22.3.x • 22.2.x	• 22.4.x • 22.3.x • 22.2.x	NA	22.3.x	• 1.23.x • 1.22.x	22.4.x	• 3GPP TS 29.510 v15.5 • 3GPP TS 29.510 v16.3.0 • 3GPP TS 29.510 v16.7

Table 3-2 (Cont.) Compatibility Matrix

CNC NF	NF Version	OCCNE	DBTier	CDCS	OSO	Kubernetes	CNC Console	3GPP
NRF	22.4.3	• 22.4.x • 22.3.x • 22.2.x	• 22.4.x • 22.3.x • 22.2.x	NA	• 22.3.x • 1.10.x • 1.6.x	• 1.23.x • 1.22.x • 1.21.x	22.4.x	• 3GPP TS 29.510 v15.5 • 3GPP TS 29.510 v16.3.0 • 3GPP TS 29.510 v16.7
NRF	22.4.2	• 22.4.x • 22.3.x • 22.2.x	• 22.4.x • 22.3.x • 22.2.x	NA	• 22.3.x • 1.10.x • 1.6.x	• 1.23.x • 1.22.x • 1.21.x	22.4.x	• 3GPP TS 29.510 v15.5 • 3GPP TS 29.510 v16.3.0 • 3GPP TS 29.510 v16.7
NRF	22.4.1	• 22.4.x • 22.3.x • 22.2.x	• 22.4.x • 22.3.x • 22.2.x	NA	• 22.3.x • 1.10.x • 1.6.x	• 1.23.x • 1.22.x • 1.21.x	22.4.x	• 3GPP TS 29.510 v15.5 • 3GPP TS 29.510 v16.3.0 • 3GPP TS 29.510 v16.7
NRF	22.4.0	• 22.4.x • 22.3.x • 22.2.x	• 22.4.x • 22.3.x • 22.2.x	NA	• 22.3.x • 1.10.x • 1.6.x	• 1.23.x • 1.22.x • 1.21.x	22.4.x	• 3GPP TS 29.510 v15.5 • 3GPP TS 29.510 v16.3.0 • 3GPP TS 29.510 v16.7
NSSF	22.4.4	• 22.4.x • 22.3.x • 22.2.x	• 22.4.x • 22.3.x • 22.2.x	NA	• 22.3.x • 1.10.x • 1.6.x	• 1.23.x • 1.22.x • 1.21.x	22.4.x	• 3GPP TS 29.531 v15.5.0 • 3GPP TS 29.531 v16.5.0 • 3GPP TS 29.531 v16.8.0 • 3GPP TS 29.501 v16.10.0 • 3GPP TS 29.502 v16.10.0
NSSF	22.4.2	• 22.4.x • 22.3.x • 22.2.x	• 22.4.x • 22.3.x • 22.2.x	NA	• 22.3.x • 1.10.x • 1.6.x	• 1.23.x • 1.22.x • 1.21.x	22.4.x	• 3GPP TS 29.531 v15.5.0 • 3GPP TS 29.531 v16.5.0 • 3GPP TS 29.531 v16.8.0 • 3GPP TS 29.501 v16.10.0 • 3GPP TS 29.502 v16.10.0

Table 3-2 (Cont.) Compatibility Matrix

CNC NF	NF Version	OCCNE	DBTier	CDCS	OSO	Kubernetes	CNC Console	3GPP
NSSF	22.4.0	• 22.4.x • 22.3.x • 22.2.x	• 22.4.x • 22.3.x • 22.2.x	NA	• 22.3.x • 1.10.x • 1.6.x	• 1.23.x • 1.22.x • 1.21.x	22.4.x	• 3GPP TS 29.531 v15.5.0 • 3GPP TS 29.531 v16.5.0 • 3GPP TS 29.531 v16.8.0 • 3GPP TS 29.501 v16.10.0 • 3GPP TS 29.502 v16.10.0
NSSF	22.4.1	• 22.4.x • 22.3.x • 22.2.x	• 22.4.x • 22.3.x • 22.2.x	NA	• 22.3.x • 1.10.x • 1.6.x	• 1.23.x • 1.22.x • 1.21.x	22.4.x	• 3GPP TS 29.531 v15.5.0 • 3GPP TS 29.531 v16.5.0 • 3GPP TS 29.531 v16.8.0 • 3GPP TS 29.501 v16.10.0 • 3GPP TS 29.502 v16.10.0
NWDAF	22.1.0	22.1.0	22.2.0	NA	NA	• 1.23.x • 1.22.x • 1.21.x	NA	• 3GPP TS 23.288 v16 • 3GPP TS 23.288 v17.4.0 • 3GPP TS 29.520 v17.6.0 • 3GPP TS 29.508 v17.5.0 • 3GPP TS 29.518 v17.5.0 • 3GPP TS 23.501 v17.5.0 • 3GPP TS 23.502 v17.4.0 • 3GPP TS 33.521 v17.1.0
SCP	22.4.4	• 22.4.x • 22.3.x • 22.2.x	• 22.4.x • 22.3.x • 22.2.x	• 22.4.x • 22.3.x	• 22.3.x • 1.10.x	• 1.23.x • 1.22.x • 1.21.x	22.4.x	• 3GPP TS 29.500 v16.6.0 • 3GPP TS 29.501 v16.5.0

Table 3-2 (Cont.) Compatibility Matrix

CNC NF	NF Version	OCCNE	DBTier	CDCS	OSO	Kubernetes	CNC Console	3GPP
SCP	22.4.3	• 22.4.x • 22.3.x • 22.2.x	• 22.4.x • 22.3.x • 22.2.x	• 22.4.x • 22.3.x	• 22.3.x • 1.10.x	• 1.23.x • 1.22.x • 1.21.x	22.4.x	• 3GPP TS 29.500 v16.6.0 • 3GPP TS 29.501 v16.5.0
SCP	22.4.2	• 22.4.x • 22.3.x • 22.2.x	• 22.4.x • 22.3.x • 22.2.x	• 22.4.x • 22.3.x	• 22.3.x • 1.10.x	• 1.23.x • 1.22.x • 1.21.x	22.4.x	• 3GPP TS 29.500 v16.6.0 • 3GPP TS 29.501 v16.5.0
SCP	22.4.1	• 22.4.x • 22.3.x • 22.2.x	• 22.4.x • 22.3.x • 22.2.x	• 22.4.x • 22.3.x	• 22.3.x • 1.10.x	• 1.23.x • 1.22.x • 1.21.x	22.4.x	• 3GPP TS 29.500 v16.6.0 • 3GPP TS 29.501 v16.5.0
SCP	22.4.0	• 22.4.x • 22.3.x • 22.2.x	• 22.4.x • 22.3.x • 22.2.x	• 22.4.x • 22.3.x	• 22.3.x • 1.10.x	• 1.23.x • 1.22.x • 1.21.x	22.4.x	• 3GPP TS 29.500 v16.6.0 • 3GPP TS 29.501 v16.5.0
SEPP	22.4.4	• 22.4.x • 22.3.x • 22.2.x	• 22.4.x • 22.3.x • 22.2.x	• 22.4.x • 22.3.x	22.3.x	• 1.23.x • 1.22.x • 1.21.x	22.4.x	• 3GPP TS 23.501 v17.6.0 • 3GPP TS 23.502 v17.6.0 • 3GPP TS 29.500 v17.8.0 • 3GPP TS 29.501 v17.7.0 • 3GPP TS 29.510 v17.7.0 • 3GPP TS 33.501 v17.7.0 • 3GPP TS 33.117 v17.1.0 • 3GPP TS 33.210 v17.1.0

Table 3-2 (Cont.) Compatibility Matrix

CNC NF	NF Version	OCCNE	DBTier	CDCS	OSO	Kubernetes	CNC Console	3GPP
SEPP	22.4.3	• 22.4.x • 22.3.x • 22.2.x	• 22.4.x • 22.3.x • 22.2.x	• 22.4.x • 22.3.x	22.3.x	• 1.23.x • 1.22.x • 1.21.x	22.4.x	• 3GPP TS 23.501 v16.7.0 • 3GPP TS 23.502 v16.7.0 • 3GPP TS 29.500 v16.6.0 • 3GPP TS 29.501 v16.5.0 • 3GPP TS 29.510 v16.6.0 • 3GPP TS 29.573 v16.3.0
SEPP	22.4.2	• 22.4.x • 22.3.x • 22.2.x	• 22.4.x • 22.3.x • 22.2.x	• 22.4.x • 22.3.x	22.3.x	• 1.23.x • 1.22.x • 1.21.x	22.4.x	• 3GPP TS 23.501 v16.7.0 • 3GPP TS 23.502 v16.7.0 • 3GPP TS 29.500 v16.6.0 • 3GPP TS 29.501 v16.5.0 • 3GPP TS 29.510 v16.6.0 • 3GPP TS 29.573 v16.3.0
SEPP	22.4.1	• 22.4.x • 22.3.x • 22.2.x	• 22.4.x • 22.3.x • 22.2.x	• 22.4.x • 22.3.x	22.3.x	• 1.23.x • 1.22.x • 1.21.x	22.4.x	• 3GPP TS 23.501 v16.7.0 • 3GPP TS 23.502 v16.7.0 • 3GPP TS 29.500 v16.6.0 • 3GPP TS 29.501 v16.5.0 • 3GPP TS 29.510 v16.6.0 • 3GPP TS 29.573 v16.3.0
SEPP	22.4.0	• 22.4.x • 22.3.x • 22.2.x	• 22.4.x • 22.3.x • 22.2.x	• 22.4.x • 22.3.x	22.3.x	• 1.23.x • 1.22.x • 1.21.x	22.4.x	• 3GPP TS 23.501 v16.7.0 • 3GPP TS 23.502 v16.7.0 • 3GPP TS 29.500 v16.6.0 • 3GPP TS 29.501 v16.5.0 • 3GPP TS 29.510 v16.6.0 • 3GPP TS 29.573 v16.3.0

Table 3-2 (Cont.) Compatibility Matrix

CNC NF	NF Version	OCCNE	DBTier	CDCS	OSO	Kubernetes	CNC Console	3GPP
UDR	22.4.2	• 22.4.x • 22.3.x • 22.2.x	• 22.4.x • 22.3.x • 22.2.x	NA	• 22.3.x • 1.10.x • 1.6.x	• 1.23.x • 1.22.x • 1.21.x	22.4.x	• 3GPP TS 29.505 v15.4.0 • 3GPP TS 29.504 v16.2.0 • 3GPP TS 29.519 v16.2.0 • 3GPP TS 29.511 v17.2.0
UDR	22.4.1	• 22.4.x • 22.3.x • 22.2.x	• 22.4.x • 22.3.x • 22.2.x	NA	• 22.3.x • 1.10.x • 1.6.x	• 1.23.x • 1.22.x • 1.21.x	22.4.x	• 3GPP TS 29.505 v15.4.0 • 3GPP TS 29.504 v16.2.0 • 3GPP TS 29.519 v16.2.0 • 3GPP TS 29.511 v17.2.0
UDR	22.4.0	• 22.4.x • 22.3.x • 22.2.x	• 22.4.x • 22.3.x • 22.2.x	NA	• 22.3.x • 1.10.x • 1.6.x	• 1.23.x • 1.22.x • 1.21.x	22.4.x	• 3GPP TS 29.505 v15.4.0 • 3GPP TS 29.504 v16.2.0 • 3GPP TS 29.519 v16.2.0 • 3GPP TS 29.511 v17.2.0

3.3 Common Microservices Load Lineup

This section provides information about common microservices and ATS for the specific NF versions in Cloud Native Core Release 2.22.4.

Table 3-3 Common Microservices Load Lineup for Network Functions

CNC NF	NF Version	Alternate Route Svc	App-Info	ASM Configuration	ATS Framework	Config-Server	Debug-tool	Egress Gateway	Ingress Gateway	Helm Test	Mediation	NRF-Client	Perf-Info
BSF	22.4.7	22.4.6	22.4.7	1.11.0	22.4.3	22.4.7	22.4.2	22.4.6	22.4.6	22.4.2	NA	22.4.4	22.4.7
BSF	22.4.5	22.4.4	22.4.5	1.11.0	22.4.1	22.4.5	22.4.2	22.4.4	22.4.4	22.4.5	NA	22.4.3	22.4.5
BSF	22.4.2	22.4.3	22.4.2	1.11.0	22.4.1	22.4.2	22.4.1	22.4.3	22.4.3	22.4.1	NA	22.4.2	22.4.2
BSF	22.4.0	22.4.1	22.4.0	22.4.0	22.4.0	22.4.0	22.4.0	22.4.1	22.4.1	22.4.0	NA	22.4.1	22.4.0
CNC Console	22.4.3	NA	NA	NA	NA	NA	22.4.2	NA	22.4.6	22.4.2	NA	NA	NA
CNC Console	22.4.2	NA	NA	NA	NA	NA	22.4.2	NA	22.4.4	22.4.2	NA	NA	NA

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

CNC NF	NF Version	Alternate Route Svc	App-Info	ASM Configuration	ATS Framework	Config-Server	Debug-tool	Egress Gateway	Ingress Gateway	Helm Test	Mediation	NRF-Client	Perf-Info
CNC Console	22.4.1	NA	NA	NA	NA	NA	22.4.1	NA	22.4.3	22.4.1	NA	NA	NA
CNC Console	22.4.0	NA	NA	NA	NA	NA	22.4.0	NA	22.4.1	22.4.0	NA	NA	NA
CNC Policy	22.4.7	22.4.6	22.4.7	1.11.0	22.4.3	22.4.7	22.4.2	22.4.6	22.4.6	22.4.2	NA	22.4.4	22.4.7
CNC Policy	22.4.6	22.4.4	22.4.6	1.11.0	22.4.1	22.4.6	22.4.2	22.4.4	22.4.4	22.4.5	NA	22.4.3	22.4.6
CNC Policy	22.4.5	22.4.4	22.4.5	1.11.0	22.4.1	22.4.5	22.4.2	22.4.4	22.4.4	22.4.5	NA	22.4.3	22.4.5
CNC Policy	22.4.4	22.4.3	22.4.2	1.11.0	22.4.1	22.4.2	22.4.1	22.4.3	22.4.3	22.4.1	NA	22.4.2	22.4.2
CNC Policy	22.4.3	22.4.3	22.4.2	1.11.0	22.4.1	22.4.2	22.4.1	22.4.3	22.4.3	22.4.1	NA	22.4.2	22.4.2
CNC Policy	22.4.2	22.4.3	22.4.2	1.11.0	22.4.1	22.4.2	22.4.1	22.4.3	22.4.3	22.4.1	NA	22.4.2	22.4.2
CNC Policy	22.4.1	22.4.1	22.4.1	22.4.1	22.4.1	22.4.1	22.4.0	22.4.1	22.4.1	22.4.0	NA	22.4.1	22.4.1
CNC Policy	22.4.0	22.4.1	22.4.0	22.4.0	22.4.0	22.4.0	22.4.0	22.4.1	22.4.1	22.4.0	NA	22.4.1	22.4.0
NEF	22.4.4	NA	22.4.7	NA	22.4.4	22.4.7	22.4.2	22.4.6	22.4.6	22.4.2	NA	22.4.4	22.4.7
NEF	22.4.3	NA	22.4.5	NA	22.4.3	22.4.5	22.4.2	22.4.4	22.4.4	22.4.2	NA	22.4.3	22.4.5
NEF	22.4.2	NA	22.4.1	NA	22.4.2	22.4.1	22.4.1	22.4.2	22.4.2	22.4.1	NA	22.4.2	22.4.1
NEF	22.4.1	NA	22.4.1	NA	22.4.1	22.4.1	22.4.1	22.4.2	22.4.2	22.4.1	NA	22.4.2	22.4.1
NEF	22.4.0	NA	22.4.0	NA	22.4.0	22.4.0	22.4.0	22.4.1	22.4.1	22.4.0	NA	22.4.1	22.4.0
NRF	22.4.4	22.4.5	22.4.7	22.4.3	22.4.3	NA	22.4.2	22.4.5	22.4.5	22.4.2	NA	NA	22.4.7
NRF	22.4.3	22.4.4	22.4.5	22.4.0	22.4.2	NA	22.4.2	22.4.4	22.4.4	22.4.2	NA	NA	22.4.5
NRF	22.4.2	22.4.3	22.4.1	22.4.0	22.4.1	NA	22.4.1	22.4.3	22.4.3	22.4.1	NA	NA	22.4.1
NRF	22.4.1	22.4.3	22.4.1	22.4.0	22.4.1	NA	22.4.1	22.4.3	22.4.3	22.4.1	NA	NA	22.4.1
NRF	22.4.0	22.4.1	22.4.0	22.4.0	22.4.0	NA	22.4.0	22.4.1	22.4.1	22.4.0	NA	NA	22.4.0
NSSF	22.4.4	NA	22.4.5	22.4.0	22.4.4	NA	22.4.2	22.4.4	22.4.4	22.4.2	NA	22.4.3	22.4.5
NSSF	22.4.2	NA	22.4.1	22.4.0	22.4.1	NA	22.4.1	22.4.2	22.4.2	22.4.1	NA	22.4.2	22.4.1
NSSF	22.4.1	NA	22.4.0	22.4.0	22.4.0	NA	22.4.0	22.4.1	22.4.1	22.4.0	NA	22.4.1	22.4.0
NSSF	22.4.0	NA	22.4.0	22.4.0	22.4.0	NA	22.4.0	22.4.1	22.4.1	22.4.0	NA	22.4.1	22.4.0
NWDAF	22.1.0	NA	NA	NA	22.4.0	NA	NA	NA	NA	22.2.0	NA	NA	NA
SCP	22.4.4	NA	NA	22.4.0	22.4.2	NA	22.4.2	NA	NA	22.4.2	22.4.3	NA	NA
SCP	22.4.3	NA	NA	22.4.0	22.4.2	NA	22.4.2	NA	NA	22.4.2	22.4.3	NA	NA
SCP	22.4.2	NA	NA	22.4.0	22.4.1	NA	22.4.1	NA	NA	22.4.1	22.4.1	NA	NA
SCP	22.4.1	NA	NA	22.4.0	22.4.1	NA	22.4.1	NA	NA	22.4.1	22.4.1	NA	NA
SCP	22.4.0	NA	NA	22.4.0	22.4.0	NA	22.4.0	NA	NA	22.4.0	22.4.0	NA	NA
SEPP	22.4.4	NA	22.4.5	22.4.0	22.4.2	22.4.7	22.4.2	22.4.6	22.4.6	22.4.2	22.4.2	22.4.4	22.4.7

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

CNC NF	NF Version	Alternate Route Svc	App-Info	ASM Configuration	ATS Framework	Config-Server	Debug-tool	Egress Gateway	Ingress Gateway	Helm Test	Mediation	NRF-Client	Perf-Info
SEPP	22.4.3	NA	22.4.5	22.4.0	22.4.2	22.4.5	22.4.2	22.4.4	22.4.4	22.4.2	22.4.2	22.4.3	22.4.5
SEPP	22.4.2	NA	22.4.1	22.4.0	22.4.1	22.4.1	22.4.1	22.4.2	22.4.2	22.4.1	22.4.1	22.4.2	22.4.1
SEPP	22.4.1	NA	22.4.1	22.4.0	22.4.1	22.4.1	22.4.1	22.4.2	22.4.2	22.4.1	22.4.1	22.4.2	22.4.1
SEPP	22.4.0	NA	22.4.0	22.4.0	22.4.0	22.4.0	22.4.0	22.4.1	22.4.1	22.4.0	22.4.0	22.4.1	22.4.0
UDR	22.4.2	22.4.4	22.4.5	22.4.0	22.4.2	22.4.5	22.4.2	22.4.4	22.4.4	22.4.2	NA	22.4.3	22.4.5
UDR	22.4.1	22.4.3	22.4.1	22.4.0	22.4.1	22.4.1	22.4.1	22.4.3	22.4.3	22.4.1	NA	22.4.2	22.4.1
UDR	22.4.0	22.4.1	22.4.0	22.4.0	22.4.0	22.4.0	22.4.0	22.4.1	22.4.1	22.4.0	NA	22.4.1	22.4.0

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	22.4.7	July 24, 2023	July 25, 2023	July 24, 2023	July 18, 2023
BSF	22.4.5	Jan 16, 2023	Jan 19, 2023	Jan 16, 2023	Jan 10, 2023
BSF	22.4.2	Jan 16, 2023	Jan 19, 2023	Jan 16, 2023	Jan 10, 2023
BSF	22.4.0	Nov 14, 2022	Nov 8, 2022	Nov 10, 2022	Nov 2, 2022
CNC Console	22.4.3	July 17, 2023	July 17, 2023	July 13, 2023	Nov 10, 2022
CNC Console	22.4.2	Apr 7, 2023	Apr 7, 2023	Apr 7, 2023	Nov 10, 2022
CNC Console	22.4.1	Nov 16, 2022	Jan 6, 2023	Jan 6, 2023	Nov 10, 2022
CNC Console	22.4.0	Nov 16, 2022	Nov 16, 2022	Nov 11, 2022	Nov 10, 2022
CNC Policy	22.4.7	July 25, 2023	July 24, 2023	July 25, 2023	July 18, 2023
CNC Policy	22.4.6	Jun 12, 2023	Jun 14, 2023	Jun 12, 2023	May 30, 2023
CNC Policy	22.4.5	Mar 14, 2023	Mar 13, 2023	Mar 08, 2023	Mar 06, 2023
CNC Policy	22.4.4	Jan 16, 2023	Jan 19, 2023	Jan 16, 2023	Jan 10, 2023
CNC Policy	22.4.3	Jan 16, 2023	Jan 19, 2023	Jan 16, 2023	Jan 10, 2023

Table 3-4 (Cont.) Security Certification Declaration

CNC NF	NF Version	Systems test on functional and security features	Regression testing on security configuration	Vulnerability testing	Fuzz testing on external interfaces
CNC Policy	22.4.2	Jan 16, 2023	Jan 19, 2023	Jan 16, 2023	Jan 10, 2023
CNC Policy	22.4.1	Nov 15, 2022	Nov 14, 2022	Nov 17, 2022	Nov 2, 2022
CNC Policy	22.4.0	Nov 15, 2022	Nov 14, 2022	Nov 17, 2022	Nov 2, 2022
NEF	22.4.4	July 18, 2023	Nov 10, 2022	July 18, 2023	Nov 10, 2022
NEF	22.4.3	Apr 4, 2023	Nov 10, 2022	Apr 4, 2023	Nov 10, 2022
NEF	22.4.2	Feb 9, 2023	Nov 10, 2022	Feb 9, 2023	Nov 10, 2022
NEF	22.4.1	Jan 11, 2023	Nov 10, 2022	Jan 11, 2023	Nov 10, 2022
NEF	22.4.0	Nov 10, 2022	Nov 10, 2022	Nov 10, 2022	Nov 10, 2022
NRF	22.4.4	July 12, 2023	July 12, 2023	July 12, 2023	July 12, 2023
NRF	22.4.3	Apr 4, 2023	Apr 4, 2023	Apr 4, 2023	Apr 4, 2023
NRF	22.4.2	Jan 18, 2023	Jan 18, 2023	Jan 18, 2023	Nov 10, 2022
NRF	22.4.1	Jan 18, 2023	Jan 18, 2023	Jan 18, 2023	Nov 10, 2022
NRF	22.4.0	Nov 10, 2022	Nov 10, 2022	Nov 10, 2022	Nov 10, 2022
NSSF	22.4.4	Apr 7, 2023	Apr 7, 2023	Apr 7, 2023	Apr 7, 2023
NSSF	22.4.2	Jan 10, 2023	Jan 10, 2023	Jan 10, 2023	Jan 10, 2023
NSSF	22.4.1	Dec 13, 2022	Dec 13, 2022	Dec 13, 2022	Dec 13, 2022
NSSF	22.4.0	Nov 11, 2022	Nov 11, 2022	Nov 11, 2022	Nov 11, 2022
NWDAF	22.1.0	Dec 6, 2022	Dec 7, 2022	Dec 7, 2022	Dec 7, 2022
SCP	22.4.4	April 11, 2023	April 11, 2023	April 11, 2023	Jan 12, 2023
SCP	22.4.3	Jan 12, 2023	Jan 12, 2023	Jan 12, 2023	Jan 12, 2023
SCP	22.4.2	Jan 12, 2023	Jan 12, 2023	Jan 12, 2023	Jan 12, 2023
SCP	22.4.1	Jan 12, 2023	Jan 12, 2023	Jan 12, 2023	Jan 12, 2023
SCP	22.4.0	Nov 29, 2022	Nov 29, 2022	Nov 29, 2022	Nov 10, 2022
SEPP	22.4.4	July 18, 2023	July 18, 2023	July 18, 2023	NA. No new APIs introduced.
SEPP	22.4.3	Apr 7, 2023	Apr 7, 2023	Apr 7, 2023	NA. No new APIs introduced.
SEPP	22.4.2	Feb 22, 2023	Feb 22, 2023	Feb 22, 2023	NA No new APIs introduced
SEPP	22.4.1	Jan 12, 2023	Jan 12, 2023	Jan 12, 2023	NA No new APIs introduced
SEPP	22.4.0	Nov 21, 2022	Nov 21, 2022	Nov 21, 2022	Nov 21, 2022
UDR	22.4.2	NA (no new security features)	March 16, 2023	March 16, 2023	Apr 5, 2023
UDR	22.4.1	NA (No new security features)	Jan 13, 2023	Jan 13, 2023	Jan 13, 2023

Table 3-4 (Cont.) Security Certification Declaration

CNC NF	NF Version	Systems test on functional and security features	Regression testing on security configuration	Vulnerability testing	Fuzz testing on external interfaces
UDR	22.4.0	NA (No new security features)	Nov 18, 2022	Nov 18, 2022	Nov 18, 2022

3.5 Documentation Pack

All documents for Cloud Native Core (CNC) 2.22.4 are available for download on SecureSites and MOS.

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

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

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

4
Resolved and Known Bugs

This chapter lists the resolved and known bugs for Cloud Native Core release 2.22.4.

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 2.22.4.

4.2.1 BSF Resolved Bugs

BSF Release 22.4.7

There are no resolved bugs in this release. The resolved bugs from 22.4.x have been forward ported to Release 22.4.7.

BSF Release 22.4.5

Table 4-1 BSF 22.4.5 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35040801	BSF response with status code 400 for pcfbinding request	When BSF receives a post request from PCF to create pcfbindings, BSF responds with a 400 error code with the reason "At least one of pcfFqdn or pcfIpEndPoints shall be included if the PCF supports the Npcf_PolicyAuthorization service."	2	22.2.5
35171745	PCF Rocklin 408 errors	JsonMappingException or ArrayIndexOutOfBoundsException reported in config-server logs during topic fetch for TopicInfo:modDate field.	2	22.3.2

Table 4-1 (Cont.) BSF 22.4.5 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35068048	Alerts on "new state : CONGESTED" and could see OutOfMemoryError on newly added diam-gateway pods	Diameter Gateway repeatedly attempts to reconnect to the peer even when reconnectLimit is set to 0 in the peer configuration during one discovery cycle.	3	22.4.0

Table 4-2 BSF ATS 22.4.5 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35040801	BSF response with status code 400 for pcfbinding request	In ATS, when either `pcfDiamHost` or `pcfDiamRealm` but not both are provided, BSF allowed to create a binding. This was happening as `pcfFqdn` is also provided.	2	22.4.0

BSF Release 22.4.2

Table 4-3 BSF 22.4.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35001007	CEA is missing few Vendor Specific Li AVP	A few supported vendors need to be published in Supported-Vendor-Id AVP during CER-CEA message exchange.	2	22.3.1

BSF Release 22.4.0

There are no resolved bugs in this release.

4.2.2 CNC Console Resolved Bugs

CNC Console Release 22.4.3

There are no resolved bugs in this release.

Table 4-4 CNC Console 22.4.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35223811	Replication issue after CNCC 22.3.1 fresh installation	The DbTier replication breaks if applications perform alter commands to modify the schema. Alter commands must not modify schema during fresh installation of CNC Console. As a resolution, Console hook changes have been made to create table schema before application startup.	2	22.3.3
35255733	Password displayed on CNCC Logs during update password	When the user updates the temporary CNCC credentials, the password is visible without masking on the CNCC Logs files. This has been resolved by adding a loggingMasks filter in the cncc-iam.ingress-gateway.log.level.cncc section in the occncc_custom_values_<version>.yaml. This fix is available in CNC Console releases 23.1.1 and 22.4.2.	2	22.4.1

Table 4-4 (Cont.) CNC Console 22.4.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35153278	CNCC cncc-mcore-igw pod taking continuously restarted after upgradation from 22.4.0 to 23.1.0 due to mismatch on requested issuer url (mCnccIams port)	The cncc-mcore-igw pod restarts repeatedly when CNC Console is upgraded from 22.4.0 to 23.1.0 This is caused by a miss match in the port. As a resolution a note has been added in the Upgrade section of the CNC Console Installation, Upgrade, and Fault Recovery Guide to ensure that the mCnccIams port configuration must be added only if port is other than 80.	3	23.1.0
35154799	The customer wants to Know the Trigger Conditions for Metrics	For cookie_routes (POLICY and BSF), Route_path is displayed as unknown and the queries and KPIs have empty results as the Route_path is unknown. As a fix for Policy and BSF, NFs' ResourcePath is used in metric KPIs and expression is updated in grafana dashboard.	3	22.2.1

Table 4-5 CNC Console 22.4.1 Resolved Bugs

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

Table 4-6 CNC Console 22.4.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34598303	CNCC IAM logs username and userId showing UNKNOWN CNCC 1.9.2	In CNCC IAM logs username and userID are showing as UNKNOWN. The username and userId of the user defaults to unknown. IAM Ingress must log the username and userId of the default user in the current log.	4	1.9.2

Table 4-6 (Cont.) CNC Console 22.4.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34752442	CNCC GUI not showing configuration done in NRF Screening Rules option.	The CNCC GUI does not show the configurations done in NRF Screening Rules option after the configurations are saved. However, API has the required configuration. This issue has been fixed.	3	22.3.0
34799529	CNCC Integration with SAML IDP Configuration missing some details in documentation.	The documentation for configuring the CNCC endpoints at SAML IDP and configuring HTTP POST binding methods at CNCC IAM was missing. The CNC Console user guide has been updated to resolve this issue.	3	22.1.0
34691804	Provide an option to use ClusterIP for LoadBalancer(LB) services.	The cluster IP is used for LB services for some specific customer deployments. The LB services are assigned LoadBalancer service type in k8s service definition. As a solution, a new flag useClusterIpForLbServices is introduced. This flag can be set to true to assign ClusterIP service type.	3	22.2.1

Note:

Resolved bugs from 22.3.1 have been forward ported to Release 22.4.0.

4.2.3 DBTier Resolved Bugs

Table 4-7 DBTier 22.4.4 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35139386	During CNDB upgrade from 22.4.1 to 23.1.0, multiple restarts can be observed in ndbmysql pods	When general query log feature was enabled in 23.1.0 during the upgrade from 22.4.1 to 23.1.0, the feature on replication SQL pod did not work, which led to continuous restart of container.	1	23.1.0
35410102	DR failure due to error: remotesitedatanodecount.properties does not exists	When the backup transfer failed and was retried, the `/var/occnedb/dbbackup/remotesitedatanodecount.properties` file was removed.	2	23.1.1
35724053	SLF/cnDBTier 22.4.3 db_tier_backup{status="FAILED"} prometheus alert	Backup failed alert was not cleared from the backup info table.	2	22.4.3
35643518	Channel switchover leading to replication break on multi channel setup	Switchover failed to resume in case of rest api timeout due to some network delay.	2	23.2.1
35740004	DBTier Installation Guide: SiteId in the yaml file need to be set as 1, 2, 3, 4	It was required to set SiteId in the yaml file as 1, 2, 3, 4 corroponding to each site as unique set identifier.	2	23.1.0
35130162	Unable to deploy a 3 or 4 site MultiChannel setup with 6 channels	The user was unable to install cnDBTier with more than 14 replication SQL pods in 3 or 4 site MultiChannel setup with 6 channels.	2	22.3.2
35789704	During rollback of CNDB from 23.2.1 to 23.1.1, replication breaks and db-backup-manager pod is stuck in crashloopbackoff	2 Hop rollback with different versions is not supported by MySQL/ cnDBTier.	2	23.1.1
35711068	22.4.3 Vertical Scaling of ndbappmysqld pods has nothing for its PVC	There was a need to add PVC vertical scaling procedure for ndbappmysqld.	3	22.4.3
35395995	Alert BINLOG_STORAGE_FULL since installing 22.3.2	BINLOG_STORAGE_FULL alert is raised if apiReplicaCount is 0 and repl sql pvc is set to 0.	3	22.3.1
35364251	DBTier 22.4.1 alert's expression issues	The descriptions of the alerts did not clearly define when the alert will get automatically cleared.	3	22.4.1

Table 4-7 (Cont.) DBTier 22.4.4 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34997129	Clarification on DBTier Automated Backup behavior	The time zone of the db-backup-manager-svc and db-backup-executor-svc had to be changed to UTC as cronitor package did not support the deployment time zone.	3	22.4.0
35590372	cnDBTier 23.2.0 MIBs and alertrules don't match	cnDBTier 23.2.0 MIBs and alertrules did not match.	3	23.2.0
35734862	Helm chart takes wrong startNodeId for ndbmysqld from custom values.yaml	The environment variable “STARTING_SQL_NODEID" was incorrectly set to “70” instead of “56” in the ndbmysqld statefulset for the init-sidecar container.	3	23.1.2
35504362	Replication svc pvc is not getting recreated on pod deletion, if in state of termination	Replication svc pvc was not recreated on pod deletion in the state of termination.	3	23.1.1
35798774	CNDBTier 23.3.0 Installation is failing via CDCS	cnDBTier installation failed while using CDCS.	3	23.3.0
35829082	REPLICATION_SKIP_ERRORS_LOW alarm is firing for cnDBTier	REPLICATION_SKIP_ERRORS_LOW alarm was raised for cnDBTier when replication halted due to skip error count less than equal to 5. Also, replication broke while performing worker node upgrade.	3	23.2.1
35372063	Skip error feature for CNDBTier not working when using site id as 5 and 6 for a 2 site GR setup	Skip Error feature was not working when using site id as 5 and 6 for a two-site georeplication setup. Instead, there was a need to add an equation to assign server id.	3	23.1.0
35432969	Listing the changes made in the CNDBTIER MOP 22.4.2 for engineering approval	There was a need to verify if the changes listed in the MOP are documented in the GA docs.	4	22.4.2

Table 4-8 DBTier 22.4.3 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35097185	During CNDB upgrade from 22.1.1 to 22.2.5, multiple restarts can be observed in CNDB pods.	Backup manager service pods restarted multiple times during an upgrade. This is a normal behavior observed when the backup manager service encounters an error. Therefore, DBTier documents are updated with notes regarding self restarts of backup manager service in case of errors.	1	22.2.5
35194625	Data loss observed along with 'Binary log cache data overflowed to disk 577 time(s). Consider increasing --binlog-cache-size' error in sql logs	The Liveness probe used the root password to query the database mysqld pods. When the root password was changed, the Liveness probe failed and the pods restarted. The dbtpasswd script was also restarting the pods simultaneously which caused the replication pods associated with a channel to be rebooted at the same time.	1	23.1.0
35193206	PROD PCF ACTIVE SESSIONS WENT DOWN to ZERO ON SOUTH LAKE due to NDB cluster restart	Replication failure was observed at customer's site. To fix the issue, configuration options are included in the values.yaml file to configure GCP monitor and LCP parameters.	2	22.3.3
35192902	PROD PCF ACTIVE SESSIONS WENT DOWN to ZERO ON SOUTH LAKE, all nDB MTD pods having one of it's containers restart	Replication failure was observed at customer's site. To fix the issue, configuration options are included in the values.yaml file to configure GCP monitor and LCP parameters.	2	22.3.2
35350673	DBTier replication failure seen during NFVI testing	Replication failure was observed at customer's site. To fix the issue, configuration options are included in the values.yaml file to configure GCP monitor and LCP parameters.	2	22.4.1

Table 4-8 (Cont.) DBTier 22.4.3 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34618463	Horizontal Scaling of ndbmtd pods	The horizontal scaling of ndbmtd pods procedure in the DBTier user guide required updates regarding the sequence to be followed while creating node groups.	2	22.3.0
35523597	cnDBTier MoP Updates:steps for ndbappmysql pod scaling with service accout and autoscaling disabled	DBTier user guide was missing steps to horizontally scale ndbappmysqld when autoscaling is disabled.	3	23.1.1
35494876	SQL pods stuck in crashloop on cndb 23.2.0 after restore with backup taken on 22.4.1	DBTier backup and restore were not supported for different DBTier versions.	3	23.2.0
35249301	Automatic restart of pod not happening when the standby ndbmysqld had a crashed binlog thread	Replication pods were not restarted automatically when the standby ndbmysqld pod had a crashed binlog thread.	3	22.4.1
35202648	DR Guide Refinement Request, re: 4-Site Geo-Replication	Fault recovery procedures in the DBTier Fault Recovery Guide required certain refinements and additional information.	3	22.4.1
35249321	Automatically purge some binlog on startup if it is full to avoid pod going in crashloopbackoff state	The binlog files were not automatically purged on startup. This caused the binlog to overflow leading to replication failures.	3	22.4.1
35116989	DBTier MIB does not comply with standard RFC2578	DBTier MIB did not comply with the RFC2578 standard.	3	22.4.1
35259935	Enhance DR logging to display the exact point and cause of failure	Customer requested for alerts when there is a failure in file transfer from one pod to other pod, or from one site to another site.	3	23.1.0

Table 4-9 DBTier 22.4.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35130162	Unable to deploy a 3 or 4 site MultiChannel setup with 6 channels.	Installation of DBTier with more than 14 replication SQL pods was not successful.	2	22.3.2

Table 4-9 (Cont.) DBTier 22.4.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35217746	NRF 23.1 cnDBTier Rollback Failure	Rollback failed while running the `hooks.sh --post-rollback` script from Bastion Host.	2	23.1.0
35207810	cnDBTier upgrade from 22.2.1 to 22.4.1 broke replication between sites	Occneuser and Occnerepluser were hard coded in the DBTier Helm chart. Therefore, when a username was created different from the occneuser or occnerepluser, it caused the replication to break during an upgrade.	2	22.4.1
35113031	GRR fails while unable to delete DB from NF nwdaf	Automated georeplication fault recovery procedure got stuck while trying to drop databases with "-" (dash) in their names.	3	22.1.1
35084355	Removing the old backups stored in the replication service in case transfer of backup failed	While performing a fault recovery, if the transfer of backup failed, then the backup had to be deleted from the replication service pod PVC.	3	23.1.0
35084371	Format SLAVE_REPLICATION_DELAY_HIGH description	Local replication service was not updating the remote backup transfer in case of failure.	3	23.1.0
35118514	Scaling procedure for ndbmtd pods does not work as expected	Fault recovery procedure had to support database restore when the data node replica counts are different from that in the remote DBTier cluster.	3	22.3.4
35182608	cnDBTier alert rules fail to load in 22.4.x due to incorrect alert indentation in cnDBTier_Alertrules.yaml file	DBTier alert rules failed to load due to incorrect indentation of BINLOG_INJECTOR_STOPPED and HEARTBEAT_FAILED alerts in the `cnDBTier_Alertrules.yaml` file.	3	22.4.2

Table 4-10 DBTier 22.4.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34623170	cnDBTier 22.3.0 ndbmysqld pod restart and replication channel stuck with error "the incident LOST_EVENTS occurred on the master. Message: mysqld startup"	DBTier 22.3.0 ndbmysqld pods restarted and the replication channel was stuck during cnPCRF upgrade with the "the incident LOST_EVENTS occurred on the master. Message: mysqld startup" error.	3	22.3.0

Table 4-11 DBTier 22.4.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34769250	GR implementation change requires updated documentation.	Request to add the following detail in the Georeplication documentation: every replication service has to communicate with every other replication service. Georeplication documentation in the Oracle Communications Cloud Native Core DBTier Installation guide has been updated with this detail.	4	22.1.3
34647888	cnDBTier PI-A 22.1.3 Helm Test logs mismatch.	Customer requested to mention the Object printed in the Helm test logs to avoid confusion.	3	22.1.3
34644803	CNE and cnDBTier 22.2.1 MIB TC textual convention files missing END statement.	The OCDBTIER-MIB-TC.MIB.txt file had a BEGIN statement but it was missing the required END statement. This issue is resolved by adding the missing END statement.	3	22.2.1
34801852	Metrics not displayed correctly for ndbinfo.operations_per_fragment and ndbinfo.locks_per_fragment tables.	Metrics were not displayed correctly for ndbinfo.operations_per_fragment and ndbinfo.locks_per_fragment tables.	3	22.3.0
34757053	cnDBTier 22.3.0 - Helm test failed for cnDBTier after successful install.	Helm test was not working when ndbmysqld replica count was 0.	3	22.3.0
34801894	handle skip errors while skipping the errors parallel in both the sites at the same time.	Request to handle skip errors while skipping the errors parallel in both the sites at the same time	3	22.3.0

Table 4-11 (Cont.) DBTier 22.4.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34648360	ndbmgmd pods keeps CrashLoopBackOff in 1.10.3 PI-D CY21.	Configure management pods (ndbmgmd) to always read the configuration from the configuration file instead of configuration cache.	3	1.10.3
34724235	NODE DOWN ALERT in PCF Production Network.	Configure management pods (ndbmgmd) to always read the configuration from the configuration file instead of configuration cache.	2	22.1.2
34770538	In ASM enabled 4 Site GR Setup for CNDB site addition, DR stuck in BACKUPRESTORE state.	New column positions mismatch between the upgrade and fresh install.	2	22.3.2
34796778	DBTier_FT_MC: On an upgraded cndb setup from 22.2.2 to 22.3.2 when upgrade is done from 22.3.2 single channel to multi channel, mysql.ndb_replication table is not existing.	mysql.ndb_replication table was not present when DBTier was upgraded from version 22.2.x to 22.3.2.	2	22.3.2

Note:

Resolved bugs from 22.3.1 and 22.3.2 have been forward ported to Release 22.4.0.

4.2.4 CDCS Resolved Bugs

Table 4-12 CDCS 22.4.2 Resolved Bugs

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

Table 4-13 CDCS 22.4.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34987684	Force installation of downloaded Python library	The default installed version of python package is not upgraded to a later release, even if the specified versions in python_libraries.txt are downloaded successfully by the retrieve_python.sh script and available on the repository.	3	22.4.0

Table 4-14 CDCS 22.4.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34505074	Incorrect syntax for exception handling in module routine SFTPPathBuilder.buildSFTPPath in cdManageArtifactRetrieval.py	The CDCS console output does not display a proper error message, "**error**", when the download-nf-release pipeline is build with the NF release that is not available in the FTP site.	3	22.2.0
34501854	Error upgrading CDCS from 22.2.x to 22.3.0	Upgrading CDCS from 22.2.x to 22.3.0 causes the following error: io.jenkins.cli.shaded.jakarta.websocket.DeploymentException: Handshake error.	3	22.2.0
34818088	CDCS DB migration script error handling for unsupported releases.	For CDCS upgrade, the current DB migration script supports only "22.3.0" as input. CDCS does not support patch or beta version. For the unsupported input other than "22.3.0" it creates the DB but fails with unhandled error as mentioned during migration:*INFO: Successfully created the Db*	3	22.3.0

4.2.5 CNE Resolved Bugs

Table 4-15 CNE 22.4.5 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36123493	OCCNE 22.4.3 Signalling LBVM Failed switchover	Manual Load Balancer Virtual Machine (LBVM) switchover left stale interfaces on the new standby LBVM. This resulted in LBVM switchover failures.	2	22.4.4

Table 4-16 CNE 22.4.4 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35560968	IPs and routes on the LBVM seem to get messed up	For some instances, IPs and routes on the LBVMs are not assigned as expected, after NF was deployed.	2	22.4.3

Table 4-17 CNE 22.4.3 Resolved Bugs

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

Table 4-18 CNE 22.4.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35082585	kubectl top nodes showing status as unknown	containerd version 1.6.4 was not compatible with Kubernetes version 1.23.7. To fix this issue, containerd version had to be updated to 1.5.8.	1	22.4.1
35145909	Deploy fails due to Not enough IPs are available for the desired node count	When deploying more than 64 nodes, the deployment failed during Kubernetes preinstall check stating "Not enough IPs are available for the desired node count".	2	• 23.1.0 • 22.4.1

Table 4-18 (Cont.) CNE 22.4.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34984839	SCP Interpod communication not working after applying Egress NAT annotations.	SCP Interpod communication was not working after applying Egress NAT annotation: oracle.com.cnc/egress-network: "sig2".	2	22.4.0
35016981	DBTier geo-replication flow in vCNE requires egress traffic on TCP ports 2022 and 3306 in LBVMs. Openstack security group is missing the egress rules to allow this flow.	cnDBTier georeplication flow in vCNE required the egress traffic on TCP ports 2022 and 3306 in LBVMs. However, OpenStack security group was missing the Egress rules to allow these ports.	2	22.4.0

Table 4-19 CNE 22.4.1 Resolved Bugs

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

Table 4-20 CNE 22.4.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34644811	Log rotation postrotate script does not work for OL8	In the provision log_config task, a postrotate script is set for the logrotate program. The postrotate script must reload the /var/log/messages and other file handles after rotation by using rsyslog, but the script was not working as expected.	3	22.1.0 22.2.0 22.3.0
33789640	OpenStack- OCCNE install adds default security group on active LBVM	OpenStack default security group was added every time an external IP address was present in the active LBVM machine along with the security group created for its local interface.	3	1.9.1 22.1.0
34650767	The addWorker.py script failed on openstack.	The addWorkerNode.py script failed to add a worker node in OpenStack.	3	22.3.0
34644755	Unable to addWorkerNode via script, "ERR: Trying to get networking information"	On running the addWorkerNode.py script, the system ran into repeated errors where the script tried and added an internal network that was already created.	1	22.3.0

Note:

Resolved bugs from 22.3.1 have been forward ported to Release 22.4.0.

4.2.6 CNC Policy Resolved Bugs

Table 4-21 CNC Policy 22.4.7 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35524791	NF_PROFILE_CHANGED messages floods towards NRF	SCP queue was filling up due to messages coming from PCF.	3	22.4.5

Note:

Resolved bugs from 22.4.x have been forward ported to Release 22.4.7.

Table 4-22 CNC Policy 22.4.6 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35530429	Post site isolation, site 2 traffic moved to site1, td-ms entry missing in site-1 and targeted traffic at site1 was not achived to 15KTPS	After the site isolation, site 2 traffic was moved to site 1. It was observed that td-ms entry was missing in site 1, and the targeted traffic of 15K Transimission Per Second (TPS) was not achieved at site 1.	2	22.4.5
35491289	Traffic getting rejected with error timeout for event: Latency: 4173ms	The diameter gateway was sending "Handling timeout event: Latency: 4173ms" message for Abort-Session-Request (ASR).	3	22.4.5
35535554	PCRF-Core is not able to apply the configuration changes to POLICYDS.REQUEST_TIMEOUT	The PCRF-Core service was not able to apply the configuration changes to POLICYDS.REQUEST_TIMEOUT.	3	22.4.5
35495581	Selective Bulk Export Giving Error "Save Failed"	While performing selective Bulk Export, if the export contains 'PeerNodeSets', then the "Save Failed" error occurred.	4	22.4.1

Table 4-23 CNC Policy 22.4.5 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35088768	PCF No New N28 message during race condition of smf CREATE & DELETE requests	When CHF Connector pod restarts during upgrade or pod boot, dataSourceRouteCtxtMap gets reset. After this, when a PUT or Delete message is received from PDS towards CHF Connector, a NPE is encountered with the data source route context being searched by fqdn.	2	22.3.3
35171745	PCF Rocklin 408 errors	JsonMappingException or ArrayIndexOutOfBoundsException reported in config-server logs during topic fetch for TopicInfo:modDate field.	2	22.3.2
35076366	CM GUI UNABLE TO LOAD ANY PROJECT IN PCF & PCRF WITH unable to write json Error	JsonMappingException or ArrayIndexOutOfBoundsException reported in config-server logs during topic fetch for TopicInfo:modDate field.	2	22.3.2
35090482	Notifications from UDR through N36 not working when Gx session contains only the MSISDN	Notifications from cnUDR to cnPCRF through N36 are not working when the Gx session contains only the MSISDN.	2	22.4.0

Table 4-23 (Cont.) CNC Policy 22.4.5 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35131946	RAR messages not being generated on Gx after Sy SNR command	When an unsupported ID given from PDS is not handled correctly, PCRF CORE showed an error and with this, breaking the flow and not triggering RAR.	2	22.4.0
35148041	pcrf-core pod in crashloopback off after 22.4.2 voice policy upgrade	*When MONITORING_PORT* in PCRF-Core deployment is not defined, it is not configurable and is hardcoded to port 9000.	3	22.2.5
35154825	CNCP BULK EXPORT not working	Bulk import does not allow file size more than 1MB to import currently.	3	22.2.6
35068048	Alerts on "new state : CONGESTED" and could see OutOfMemoryError on newly added diam-gateway pods	Diameter Gateway repeatedly attempts to reconnect to the peer even when reconnectLimit is set to 0 in the peer configuration during one discovery cycle.	3	22.2.5
35158666	Policy Alert "DiamEgressErrorRateAbove1Percent" references response code which is not present	Sy related metrics in Diameter Connector was not correctly implemented.	4	1.15.0

Table 4-23 (Cont.) CNC Policy 22.4.5 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35176575	PCF sending empty header packet to BSF after 22.3.3 Upgrade	When BSF registration fails, it isn´t having location header saved in the DB. When delete comes, there is no validation whether BSF registration was successful which results in setting 3gpp-sbi-target-apiroot as [[null://null]].	4	22.3.3
35191581	Session state variable(s) not working as expected	In PCRF-Core, it is not possible to store something that is not a string inside session state variables.	4	22.4.1

Table 4-24 CNC Policy ATS 22.4.5 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35131946	RAR messages not being generated on Gx after Sy SNR command	When unsupported ID given from PDS is not handled correctly, PCRF-Core showed an error and with this, breaking the flow and not triggering RAR.	2	22.4.0

Table 4-25 CNC Policy 22.4.4 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35060470	URSP Uninstall Failure	The PCF user service does not uninstall URSP rules as determined by the PRE service.	1	22.4.2

Table 4-25 (Cont.) CNC Policy 22.4.4 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35058176	PCF is not evaluating the RS-Bandwidth and RR-Bandwidth as 0 in AAR Request RX call	The issue with PCF in sending maxUl/Dl and gbrUl/Dl BW values for RTCP flows when it is not evaluating the RS-Bandwidth and RR-Bandwidth as 0.	2	22.4.1

Note:

Resolved bugs from 22.3.x have been forward ported to Release 22.4.4.

Policy ATS 22.4.4

There are no resolved bugs.

Table 4-26 CNC Policy 22.4.3 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35028167	PCF Rx LI-Indicator not passed on to SMF	PCF received the Rx AAR with LI-Indicator, but did not send it to the SMF.	2	22.4.1

Note:

Resolved bugs from 22.3.x have been forward ported to Release 22.4.3.

Policy ATS 22.4.3

There are no resolved bugs.

Table 4-27 CNC Policy 22.4.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35001349	URSP rule getting rejected due to formatting error	URSP rule gets rejected due to formatting error. Hence, update the N1 message encoding or decoding format of URSP for SNSSAI Route Descriptor Type as per spec version 16.2.	1	22.4.1
35001007	CEA is missing few Vendor Specific Li AVP	A few supported vendors need to be published in Supported-Vendor-Id AVP during CER-CEA message exchange.	2	22.3.1
35007611	PCF GUI forcing entry of optional field while creating URSP rule	Under Route selection Descriptor Component in the type “SNSSAI,” all the other required fields need to be removed except SST.	2	22.4.1
34974815	SNR not processed by CNCP as a result incorrect PCC ruledelivered by CNCP for the data apn session	In a multisite setup, PDS does not update the last modified time while updating the OCS notification changes to the PDS DB due to which notification changes are not picked by another site.	2	22.3.2

Table 4-27 (Cont.) CNC Policy 22.4.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34964990	UE Policy Message Size shall support bigger range	UE Policy Message Size supports a bigger range. Hence, the size for n1MsgTransferSettings is changed from 0-9000 to 14-65535, whereas the size of uePolicySectionMaxSize is changed from 0-9000 to 4-65528.	3	22.4.0
34984926	pds pre-install pod fails upgrade from 22.3.0 to 22.4.0	MySQL copy algorithm being used to set the default value when records are available in the table causes concurrent DML operation. This further causes the DDL statements to fail and leads to changes in data in the source table during the ALTER TABLE copy process.	3	22.4.0

Note:

Resolved bugs from 22.3.x have been forward ported to Release 22.4.2.

Policy ATS 22.4.2

There are no resolved bugs.

Table 4-28 CNC Policy 22.4.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34855517	PCF not able to send Rx rules in UpdateNotification to SMF	When Rx AAR has four subcomponents that include two audio and two video components, the PCF does not send UpdateNotify to SMF.	1	22.3.3
34869914	URSP message formatting	The UE Policy section management list IEI should be included in the 'Manage UE Policy' command. The UE is not able to interpret the current 'Manage UE Policy' command from PCF.	2	22.3.3
34809747	pcrf-core sends incorrect location variable to pre, causing incorrect policy evaluation	A policy rule is failing intermittently in PCRF-core calls due to the location session variable value not getting success a few times in Gx RAR messages.	3	22.3.1

Note:

Resolved bugs from 22.3.x have been forward ported to Release 22.4.1.

Policy ATS 22.4.1

There are no resolved bugs.

Table 4-29 CNC Policy 22.4.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
34659822	PCF prod IODT: Errors were observed on PCF diam-connector pods	When AAR is sent with more than one media component and if the subcomponent is missing, the request is failed and 5012 is sent.	2	22.1.1
34779369	PCF 503 Errors due to BSF Target API root header showing NULL	Binding pod is setting "3gpp-sbi-target-apiroot=[null://null]" and thereby 503 Errors are being observed.	2	22.3.2
34716980	Alternate service pod traffic distribution is inconsistent	During BM testing, it is observed that when a retry profile is enabled and traffic is running at 14K TPS, the alternate service pod keeps rebooting. On analysis, it was found that the pod reboot reason was exit code 137, which was due to resource shortage.	2	22.3.0
34760967	Unable to Deploy/Upgrade Policy using node-selectors	By adding the global NodeSelector values, all pods are not added with nodeSelector. Only two pods are added with np=pcf.	2	22.2.3
34727498	DIAMGW is not responding after couple of hours	Diameter Gateway does not respond for couple of hours as there is no response for TCP SYN Message from Simulator.	2	22.3.0

Table 4-29 (Cont.) CNC Policy 22.4.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
34725424	monitoredResourceUris change in PUT message	f PCF triggers PUT towards the UDR, the following UDR on-demand discovery is triggered due to SM_create: 1. SM_create (dnn1) arrives, and subscription on UDR-1 is created. 2. SM_create (dnn1) again arrives, refetch functionality triggers, and sends UDR PUT with monitored resource uri to be same as target root API. 3. SM_delete arrives. The session is cleaned. No delete is sent towards UDR/ CHF(as this may not be the last session). 4. *SM creates again comes. UDR on-demand discovery happens.* 5. PCF this time picks UDR-2 to fetch sm-data. 6. PCF triggers PUT for udr subscription (on existing	2	22.2.3

Table 4-29 (Cont.) CNC Policy 22.4.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
		subscription-id) however monitored resource uri is modified along with new target api - of UDR2. The expected behavior is PCF should not change monitored resource uri even if the target-api-root is changed to UDR-2.		
34644466	PDS is forwarding to PCRF-Core notify UDR data with different structure	When UDR triggers a notification to cnPCRF, the data received in PDS has a different structure format.	2	22.3.0
34693343	race condition encountered in UDR when ims and internet subscription happens together	During the race condition with Bulwark service is disabled, PCF does not delete the stale subscription to UDR.	3	22.3.0

Note:

Resolved bugs from 22.3.1 and 22.3.2 have been forward ported to Release 22.4.0.

Policy ATS 22.4.0

There are no resolved bugs.

4.2.7 NEF Resolved Bugs

OCNEF Release 22.4.4

There are no resolved bugs in this release.

OCNEF Release 22.4.3

Table 4-30 OCNEF 22.4.3 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35142862	In in-service upgrade of NEF from 22.4.1 to 23.1.0, aef-apirouter pods are not coming up	The aef-apirouter pods are not coming up in-service upgrade of NEF from 22.4.1 to 23.1.0.	2	22.4.1

OCNEF Release 22.4.2

Table 4-31 OCNEF 22.4.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35062697	NEF - PCF Media-Type parameter is needed to support successful AFSessionwithQOS initial setup	NEF supported `AFSessionWithQOS` procedure supports the "Media-Type" parameter in the `Npcf_policyAuthorization` API. This parameter is mandatory to have a successful AF Session in QoS procedure with PCF.	3	22.4.1

OCNEF Release 22.4.1

There are no resolved bugs in NEF Release 22.4.1.

OCNEF Release 22.4.0

There are no resolved bugs in NEF Release 22.4.0.

4.2.8 NRF Resolved Bugs

Table 4-32 NRF 22.4.4 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
35417814	Discovery Cache is not refreshing records for Custom NFs.	Discovery Cache was not refreshing records for Custom NFs. **Note**: Backported from 23.2.0.	3	23.1.1

Table 4-32 (Cont.) NRF 22.4.4 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
35286843	Error code 503 is observed across all NRF operations during 12K TPS performance run on each site.	Error code 503 was observed across all NRF operations during 12K TPS performance run on each site. **Note**: Backported from 23.2.0.	2	23.1.0

> **Note:**
> Bugs from 22.3.2 release are already ported to release 22.4.4.

NRF 22.4.3 Resolved Bugs

There are no resolved bugs in this release.

Table 4-33 NRF 22.4.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
35131679	NF Discovery forwarding returning empty response	When NF Discovery forwarding happens to another NRF and second NRF not returning suspended NF profiles with empty list feature enabled.	3	22.4.1

> **Note:**
> Bugs from 22.3.2 release are already ported to release 22.4.2.

Table 4-34 NRF 22.4.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
34848384	NRF Auditor Microservice issues when connectivity between NRF and DB is down	The auditor microservice pod restart is observed after DB connectivity is restored.	3	22.4.0

Table 4-34 (Cont.) NRF 22.4.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
34848377	NRF Configuration Microservice issues when connectivity between NRF and DB is down	The configuration microservice pod continuously restarts when DB connectivity is down.	3	22.4.0

Note:

Bugs from 22.3.2 release are already ported to release 22.4.1.

Table 4-35 NRF 22.4.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
34839907	OCNRF Roaming MNC with 2 digits is treated as different with 3 digits when leading 0 value.	OCNRF Roaming works differently when MNC is 2 digits and 3 digits, with the leading 0 value in MNC. For example: MCC- 310 and MNC - 14 is treated different when compared with MCC-310 and MNC-014.	3	22.3.1
34824546	SLF03_discovery_slf_query and Subs03_with_NotifCondition test cases failed during the nightly run	SLF03_discovery_slf_query and Subs03_with_NotifCondition test cases failed during the nightly run. Issue was with communication between Stub and ATS due to third-party library code.	3	22.3.1

Table 4-35 (Cont.) NRF 22.4.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
34837622	OCNRF Roaming needs to relax check of requester attributes when Roaming flag is disabled	OCNRF Roaming needs to relax check of requester attributes when Roaming flag is disabled. When requester PLMN specific attributes are received at OCNRF and Roaming is disabled, OCNRF was rejecting the request. Checks are relaxed for such scenarios in AccessToken and Subscription.	3	22.3.1
34799340	NRF configuration pod stuck in 1/2 state during NRF Fresh installation on 22.4.0-rc3. NRF config pod restart required	NRF configuration pod stuck in 1/2 state during NRF fresh installation on 22.4.0-rc3. t is required to restart the NRF configuration pod.. Due to some thread synchronization issue during startup of NRF Configuration, pod was not coming up.	2	22.3.1
34699360	NF is not moving into Suspended state from Probable-suspended even when HB is stopped and Replication is up	NF is not moving into Suspended state from Probable-suspended, even when HB is stopped and Replication is up.	2	22.3.0
34721036	NWDAF registration errors for optional attributes	NWDAF registration is failing with errors for optional attributes such as analyticsDelay, nwdafCapability.	2	22.3.0
34653278	NRF-EmptyList_FT:NRF-Discovery not sending NF profiles of Suspended NF when Forwarding is enabled but Rule is not configured	NRF-Discovery is not sending NF profiles of Suspended NF when Forwarding is enabled but Forwarding Rule is not configured.	3	22.3.0

Table 4-35 (Cont.) NRF 22.4.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
34644919	Duplicate microService unavailability alert and Alert description is not matching alert behavior	Alert should be raised when microservice is completely down and no replicas are available. Alert is raised even if some, not all replicas are going down. Replicas are still available. Also, duplicate alerts are raised.	3	22.1.0
34426591	NRF not sending DNS update for already Registered AMFs after Enabling DNS feature	NRF does not send NAPTR updates for the AMFs that are registered when the DNS NAPTR feature is disabled. NRF sends DNS updates for already Registered AMFs after enabling DNS feature.	3	22.2.0
34545093	NF_Register Request with nfProfileChangeInd not compliant	NF_Register Request is not compliant with nfProfileChangeInd. If NRF configured PLMN say MCCMNC 208-01 and in nfProfile registration, 208-01 and 206-01. NRF saves nfProfile with 208-01 only, but in the response NRF is not informing to consumer that 208-01 is only accepted when nfProfileChangeInd is true.	3	22.2.0
34426530	NRF-DNS NAPTR Record not completely cleaned up from DNS after AMF-NF De-registration	NRF-DNS NAPTR record is not completely cleaned up from DNS after AMF-NF De-registration. When different AMFs are sharing the amfName, amfSetId, amfRegionId, then deregistration of AMF is not cleaning the records in NAPTR properly.	3	22.2.0

Table 4-35 (Cont.) NRF 22.4.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
34426552	NRF not removing DNS records for Registered AMFs after switching DNS feature flag to Disabled	When DNS NAPTR feature is disabled, NRF must remove the DNS NAPTR records from DNS server. This is done once the feature is disabled. DNS NAPTR records shall become stale and outdated information is accessed.	3	22.2.0
34473746	NRF ocnrf_stale_nfSubscriptions_deleted_total metrics not getting pegged	NRF ocnrf_stale_nfSubscriptions_deleted_total metrics is not pegged.	4	22.1.0
34205693	Complete removal of ipv4EndpointAddress or ipv6EndpointAddress in n2InterfaceAmfInfo is not resulting in removal from DNS Server	Complete removal of ipv4EndpointAddress or ipv6EndpointAddress in n2InterfaceAmfInfo does not remove them from DNS Server.	3	22.2.0
34205878	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.	3	22.2.0
34185802	NRF is not raising Alert "OcnrfMaxSlfAttemptsExhausted" upon SLF failure. Metric is also not visible in Prometheus	NRF is not raising Alert "OcnrfMaxSlfAttemptsExhausted" upon SLF failure. Metric is also not visible in Prometheus.	4	22.1.0
34847444	Overload control misconfiguration causing flooding warn log	Overload control misconfiguration causing flooding warn log.	3	22.3.1

4.2.9 NSSF Resolved Bugs

NSSF 22.4.4 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35052433	NSSF is not sending subscription request message after timer-expiry	The below parameter was configured in the ocnssf-22.4.2.0.0.custom-values.yaml file: *renewalTimeBeforeExpiry=60* While adding the Amf-set in CNCC, NSSF sends a discovery message to NRF to get all active AMFs in an AMF-set. NSSF should send the subscription request to NRF for configured Amf-set. As per the above configuration, NSSF should renew the subscription request after 60 seconds, but NSSF is not sending the subscription request after 60 seconds.	2	22.4.2

Bug Number	Title	Description	Severity	Found in Release
35195268	Issue with the NSSF ATS deployment.yaml file	There are following issues in the NSSF ATS package with PVC enabled: 1. NSSF-ATS 23.1.0: ocnrf_tests folder present in NSSF ATS pod. Only the ocnssf_tests folder is expected in the ATS pod but an extra folder named ocnrf_tests is also present. 2. Wrong heading in NSSF ATS GUI. 3. Files present in the ocnssf_tests folder in the ATS pod. 4. Error: Inside the tgz file at the below location and line numbers 72 & 73, we have parameters with ocnrf_tests, which is creating a mount path in volume with ocnrf_tests folder.	3	22.3.0
34874721	NSSF ATS 22.3.0 Health check failure	The health check test in ATS is failing for release 22.3.0.	3	22.3.0
35250829	The "serviceAccountName" parameter missing in ATS values yaml file	The "serviceAccountName" is to be added in the ocats-nssf-custom-values.yaml file so that installation can use existing service agreement in the lab.	3	22.4.3
35022513	NSSF is sending incorrect targetNfType in discovery message towards NRF	NSSF is sending incorrect `targetNfType` in the discovery message towards NRF.	3	22.4.2

NSSF 22.4.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34903450	NSSF-ATS 22.4.1 | Testcases in regression are getting failed	Intermittent failure in NSSF ATS test cases.	3	22.4.1
34931525	Secret Name issues in NSSF Installation document	Secret Name issues in NSSF Installation document	3	22.4.1
34940152	No match for role binding" for ingress-gateway while upgrading NSSF version V22.3.1 to V22.4.1	Facing issues with the preupgrade hook in Ingress Gateway while upgrading NSSF 22.3.1 to NSSF 22.4.1.	3	22.4.1

Table 4-36 NSSF 22.4.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34871318	NSSF ATS OAuth testcases failing	NSSF ATS OAuth test cases were failing due to the following issue with the certificates: NSSF-ATS uses preconfigured keys in the certificates for validation of the OAuth test cases. The autogenerated keys do not match with the preconfigured keys, thus failing the test cases. To solve this, Readme file and the Cloud Native Core Network Slice Selection Function Installation and Upgrade Guide were updated with the steps for creating the keys and applying preconfigured tokens to them. These preconfigured keys can be used in NSSF-ATS to run the test cases successfully.	3	22.4.0

Table 4-37 NSSF 22.4.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34815361	NsSelection request responding for a requestmapping Call with HTTP 500 when candiateAMF is also enabled	NSSF is responding with 500 for request mapping when the request mapping flag is set to true and candidate resolution is also enabled.	3	22.3.0

4.2.10 NWDAF Resolved Bugs

NWDAF 22.1.0 Resolved Bugs

There are no resolved bugs.

4.2.11 SCP Resolved Bugs

Table 4-38 SCP 22.4.4 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35697189	Content Type being changed by SCP to PCF	SCP was changing Content Type for the error response received from producer NF to application/problem+json.	2	22.3.2

Table 4-39 SCP 22.4.3 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35279530	SCP Model-D performance degradation observed.	SCP was sending a GOAWAY frame even if the HTTP/2 connection had traffic causing traffic degradation.	3	22.4.0
35279502	Prometheus restart observed due to high number of samples.	Enables or disables the use of dimensions such as "ocscp_nf_instance_id" and "ocscp_service_instance_id" that can be configured.	3	22.2.2
35279496	SCP is not sending its own LCI while sending the response from interSCP to unknown peer	SCP was not sending its own LCI while sending the response from interSCP to an unknown peer.	3	23.1.0
35279485	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 cases, therefore the related alerts are dependent on this metric.	3	22.2.2

Table 4-39 (Cont.) SCP 22.4.3 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35182545	OutlierDetection confirguration failing with code 403 for put operations	SCP was occasionally sending 400-bad requests when service-specific discovery was enabled for delegated discovery.	3	22.4.2
35249225	SCP taking NF FQDN as null from NFProfile in Model-D https call when IpEndpoints and FQDN is null at service level	SCP considered NF FQDN as null from NFProfile in Model-D https call when IpEndpoints and FQDN were null at service level.	3	22.4.0
35279465	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
35279447	SCP intermittently fails to forward NF Deregistration notification request to AMF	TCP retransmissions were observed because peers were not responding with TCP acknowledgement. Instrumentation was added to get more data for debugging.	3	22.2.2
35219580	ATS New Features OutlierDetectionInterSCP Feature Failure is observed.	The scenario was not simulating the timeout correctly. The feature file was updated to simulate timeout, and validations were updated accordingly.	2	22.4.2
35141893	Notification processing failure resulting in resource mapping deletion in some exception cases.	Restore a deleted resourceMappings for rel15 rule processing when there is an exception during Notification processing.	3	22.2.2
35279406	Egress_congestion_based_on_producer_load_and_message_priority_UDM Scenario-8 failed	ATS is enhanced to check whether a notified profile is updated in database at a later time or not, rather than checking in the last 30 seconds.	3	23.1.0

Table 4-40 SCP 22.4.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35011159	Alternate-resolution pod restarts when DNS queries timeouts continuously	The Alternate-resolution pod restart was observed when DNS queries timeouts continuously as thread watchdog identifies DNS thread to be stuck.	2	22.4.1

Table 4-40 (Cont.) SCP 22.4.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35028366	Inter Microservice resiliency not working for scp-worker	Inter microservice resiliency was not working for scp-worker as service port was hardcoded.	2	22.4.1
35008662	Upgrade to 22.4.0/22.4.1 does not create NF Profile rule when it receives Registration notification from NRF	Upgrade to 22.4.0 or 22.4.1 does not create NF Profile rules when it receives Registration notification from NRF.	2	22.4.0
35001956	Generated 3gpp-sbi-target-apiroot includes trailing slash / if path pseudo-header not in UDM response	Removed Trailing slash from SCP added 3gpp-sbi-target-apiroot header in case of Dest-Reselection for modelC and modelD response to consumer NFs.	3	22.3.0
35004972	When a producerNF is unavailable, SCP does not attempt alternate routing and instead returns a 400 error with the incorrect cause	SCP was occasionally sending 400 bad request when service specific discovery was enabled for delegated discovery.	3	22.4.0
35017109	After setting the logging level to INFO/WARN still the pods show DEBUG logging level	The Log level of few packages was not getting reverted when SCP is deployed with DEBUG Log levels.	3	22.4.0
34971110	SCP R15 reverse proxy rules get deleted and are not safeguarded when parallel processing of profiles from configuration module (SCP and NRF)	SCP rel15 reverse proxy rules are removed and are not protected when parallel processing of profiles from the configuration module (SCP and NRF).	3	22.2.2
35036132	Audit, Notification, and Subscription pod restarted on SCP during the DBTier upgrade	DB connection timeout was causing SCP microservices to restart. Fixed the issue so that service does not restart on db connection failure.	3	22.4.0
35061867	GlobalEgressRateLimiting.feature scenario is failing	Scenario was modified to update validation for metric ocscp_metric_egress_rate_limiting_not_applied_req_total in rate limiting scenarios.	3	22.4.1
35067260	ATS Feature Ingress_Rate_Limiting_enhancement_for_nfInstanceId_to_support_UserAgentHeader failing	Scenario was fixed to remove unnecessary alert validations in the Ingress_Rate_Limiting_enhancement_for_nfInstanceId_to_support_UserAgentHeader feature file.	3	22.4.1

Table 4-40 (Cont.) SCP 22.4.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35057152	OutlierDetectionInterSCP feature is failing in New-feature pipeline	Additional wait was added to one of the scenarios to fix the issue.	3	22.4.1
35067318	After Alert_SCPIngressTrafficRateExceededConfiguredLimit-Scenario 3 Failure and others need retry	Maximum wait time for retries is increased to avoid issues due to latency.	4	22.3.2

Table 4-41 SCP 22.4.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34945407	SCP adds content-length as 0 in the response that SCP relays on the downstream path	SCP adds content-length as 0 in the response that SCP relays on the downstream path.	2	22.3.0
34933487	ATS 22.4.0 Connection failure for the STUBS	ATS 22.4.0 connection fails for the stubs.	2	22.4.0
34945946	ocscp nf load metrics are showing an incorrect load value for other registered NF's	OCSCP NF load metrics display an incorrect load value for other registered NFs.	3	22.4.0
34951564	Unexpected behavior of go-stubs while trying deployment using combined ATS charts	Unexpected behavior of go-stubs while trying deployment using combined ATS charts.	3	22.4.0
34864506	OD functionality for SEPP is not working because of dependency of SEPP OD audit on SCP config	The Outlier Detection (OD) functionality for SEPP is not working due to dependency of SEPP OD audit on SCP config.	3	22.4.0
34866248	SCP Local Rate Limit does early rejections of messages compared to configured rate	SCP Local Rate Limit performs early rejections of messages as compared to configured rate limit.	3	22.4.0
34945811	Callback notification messages routing from NF producer to NF consumer not working correctly in reverse proxy	Callback notification messages routing from producer NF to consumer NF are not working in reverse proxy.	3	22.4.0

Table 4-41 (Cont.) SCP 22.4.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34872096	Values not matching Data types in CSAR package yml file	Values are not matching the Data types in the CSAR package yaml file.	3	22.4.0
34967681	SCP does not match routing rule when 3gpp-sbi-target-apiroot contains capital letters	SCP does not match routing rule when the 3gpp-sbi-target-apiroot header contains capital letters.	3	22.3.0
34930495	PVC is not getting attached to in the ATS Pod	PVC is not getting attached to in the ATS pod due to Helm chart issue.	3	22.4.0
34944861	scp CSAR file Definitions/ocscp.yaml file has invalid yaml	The SCP CSAR file Definitions/ocscp.yaml file has invalid yaml.	3	22.3.0
34919781	Enhanced_NF_Status_Processing_UNDISCOVERABLE scenario failure	Configuration clean up was missing in one the scenarios causing intermittent failure.	3	22.3.2
34939704	Message Copy feature in SCP not including response code received from producer in header list	The Message Copy or Traffic Feed feature in SCP does not include response codes received from producer NFs in the header list.	4	22.4.0
34842720	Worker logs generating exception when setting the worker Log Level as DEBUG	Worker logs are generating exception when setting the worker Log Level as DEBUG.	4	22.4.0
34976237	scp-worker response processing time is not showing correct values in case of timeout error in Model D call flow	scp-worker response processing time is not showing correct values in case of timeout error in Model D call flow.	4	22.4.0

Table 4-42 SCP 22.4.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34387842	Downstream connections idleTimeout is not graceful & not present in ocscp_values.yaml	HTTP idleTimeOut value for downstream connections were missing in deployment file and SCP was not sending GOAWAY on downstream connection before connection termination.	3	1.15.3

Table 4-42 (Cont.) SCP 22.4.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34513191	Getting an empty array for Routing Rules query with nfType "5G_EIR"	NFType is incorrectly mapped in SCP for 5G_EIR causing empty array for Routing Rules query with nfType "5G_EIR".	3	22.1.2
34575128	SCP registration to NRF fails when scheme is set to https	SCP was not using default https port of NRF for requests towards NRF, when NRF profile under service level has scheme as https and endpoints are commented.	3	22.3.0
34607486	vSCP does not add via header if the error is generated by hSCP	SCP was not adding via header with scp fqdn in case of error response relayed by SCP.	3	22.3.0
34612744	Metric <ocscp_metric_egress_rate_limiting_throttle_req_total> of EgressRateLimiting.feature, scenario-3 needs to have tolerance	Metric <ocscp_metric_egress_rate_limiting_throttle_req_total of EgressRateLimiting.feature, scenario-3 must have tolerance.	3	22.2.1
34641640	SCP ATS - 22.3.0 - Need clarification on customizing test cases	Custom directories were missing in ATS package.	3	22.3.0
34758360	SCP Data Feeder Does Not Publish GET Query Parameters to DD Kafka Topic	SCP was not sending query parameters in :path header to trafficfeed causing query parameters not being published to kafka.	3	22.3.0
34711102	Enhanced_Suspended_State_Routing_Model_C_Inter_SCP is failing during individual run.	Testcase failed due to incorrect feature configuration. Steps in the feature file are corrected to fix the issue.	3	22.3.0
34657637	ForeignNFLocalityNotServed" alarm not clearing after issue is resolved	"ocscp_notification_foreign_nf_locality_unserved" is pegged when a NF register with locality is not served by any SCP, but the metric is not cleared when the NF deregisters.	3	1.15.2
34646634	SCP swagger UI shows multiple Ingress Rate Limiter options	SCP swagger UI shows multiple Ingress Rate Limiter options - Ingress Rate Limiter Info and Ingress Rate Limiter.	4	22.3.0

Table 4-42 (Cont.) SCP 22.4.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34618123	Exclude ports like (8091) by defaultin outer ocscp_values.yaml	By default port 8091 was not excluded in deployment file causing failure to fetch metrics if SCP is deployed with a side car. Annotations were enabled to exclude the port 8091 from the deployment file.	4	22.1.2
34589571	CNCC GUI does not show service level priority for retrieved NF profiles	CNCC GUI does not show service level priority for retrieved NF profiles.	4	22.1.0
34570381	Update the rest api doc with correct example for egress rate limiting configuration, wherein payload json should have "rate" instead of "reservedRate"	Update the rest api doc with correct example for egress rate limiting configuration, wherein payload json should have "rate" instead of "reservedRate"	4	22.2.0
34569501	Endpoint 8010 from cache service needs to be removed, as its not implemented for its use	Endpoint 8010 from cache service needs to be removed, as it's not implemented for use.	4	22.1.2
34504868	SCP does not respond with the correct error cause if the trigger point or rule name parameter is missing	SCP responded with the error cause "MANDATORY_IE_INCORRECT" instead of "MANDATORY_IE_MISSING" if the trigger point or rule name parameter is missing.	4	22.3.0
34348061	There is no proper reporting of error details when maximum match blocks exceed the limits in SCP	There is no proper reporting of error details when maximum match blocks exceed the limits in SCP.	4	22.2.0
34235123	SCP is not validating messageType parameter while creating new rule for SBI Message Priority	SCP is not validating messageType parameter while creating new rule for SBI Message Priority.	4	22.2.0
34235110	In the discovery statistics for Explicit Notification, there is an inconsistency in the value of the ocscp_nf_service_type parameter	In the discovery statistics for Explicit Notification, there is an inconsistency in the value of the ocscp_nf_service_type parameter.	4	22.2.0
34235069	Status parameter in HTTP response body doesn't seem to be consistent	An error cause was displayed along with status code for some error responses.	4	22.1.2

Table 4-42 (Cont.) SCP 22.4.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34148964	SCP does not validate the httpMethods parameter value before applying the SBI rules	SCP does not validate the httpMethods parameter value before applying the SBI rules.	4	22.1.2
34818917	Duplicate record "nudr-dr" in SCP Configuration -> Routing option configuration	Duplicate record "nudr-dr" in SCP Configuration -> Routing option configuration	4	22.3.0
34797551	Scenario 2 of Alert_SCPEgressTrafficRateExceededConfiguredLimit feature failing in individual run	The SCPEgressTrafficRateExceededConfiguredLimit alert was failing due to configuration step missing in testcase.	4	22.3.1

Note:

Resolved bugs from 22.3.2 have been forward ported to Release 22.4.0.

4.2.12 SEPP Resolved Bugs

SEPP 22.4.4 Resolved Bugs

There are no resolved bugs in this release.

SEPP 22.4.3 Resolved Bugs

There are no resolved bugs in this release.

Table 4-43 SEPP 22.4.3 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35208657	DBTier_Rollback: SEPP Pods restart leading to missing SEPP tables post CNDB rollback from 23.1.0 to 22.4.0 causing complete traffic failure	Few tables are removed from SEPPDB during the cnDBTier rollback from 23.1.0 to 22.4.0 resulting complete traffic failure. SEPP pods cn32f and pn32f restarted during the cnDBTier rollback. This occurs when config-mgr-svc is restarted after cnDBTier rollback. This is due to an issue that alter table command that is used to update the Dbengine to NDBcluster (for CNE setup). As a fix, the alter table command usage is removed from config-mgr-svc code.	3	22.3.0
35211643	SEPP Upgrade & Install: SEPP pods deployment edit required for OSO integration after SEPP fresh install and upgrade	After doing the steps for SEPP integration with OSO during SEPP installation and upgrade, SEPP deployment must be edited . As a result of the edit, SEPP pods restart. This impacts the upgrade. As a fix, the following changes are integrated: oracle.com/cnc: \"true\ is changed to oracle.com/cnc: "true" Extra characters are not getting replaced. As a result, the user has to edit the service the remove them.	3	22.3.0
35126068	Re-init field is updated to N32F_ESTABLISHED_STATE at the producer side	Added the details in SEPP REST API about re-init field and the corresponding allowed state.	4	22.4.0

Table 4-44 SEPP 22.4.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35104190	Rollback failed from 23.1.0 to 22.4.1	SEPP rollback failed from 23.1.0 to 22.4.0 and 22.4.1. As the namespace tag was missing in ASM charts which had an impact on both ASM and non-ASM setup.	3	22.4.0

Table 4-45 SEPP 22.4.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34533995	RemoteSEPP Delete REST API at config mgr returns success incase underlying failures	Deleting RemoteSEPP REST API at config mgr returns success in case of failure also. RemoteSEPP remains in database even after running delete command. It happens randomly and not for all the cases.	4	22.3.0
34892299	Latency metric corrections required in user guide	Some of the metrics dimensions are different in user guide and code. Updated the user guide to make it consistent.	4	22.4.0
34939411	RemoteSEPPSet Creation Error via CNCC after P-RSS enabled	If Hosted SEPP is deployed and P-RSS is enabled through CNC Console GUI, creating Remote SEPP returns an error. This is because the json file which is used to load the menu on CNCC has not coded completely. Updated the json file for all the features.	3	22.4.0
34838242	SEPP-Upgrade: TH is disabled after upgrade from 22.3.0 to 22.4.0	If topology hiding (TH) is enabled in 22.3.x release, the topology hiding was getting disabled by default after upgrading to 22.4.0. This is because TH enable disable functionality is moved to a different table in 22.4.0 which was not behaving as expected. After the fix, if topology hiding is enabled, it remains enabled after upgrade and if disabled, it remains disabled after upgrade.	3	22.4.0
34745796	SEPP-PERF: Some correction require in Grafana graph heading showing in milli second(ms) and value in traffic instead of second(s)	Some correction is required in the Grafana graph heading, which is showing values in milli seconds instead of seconds. 1. CN32F processing time graph heading showing the values in ms. 2. PN32F processing time graph heading showing the values in ms and value of min, max, and, avg showing inMillion. 3. IGW processing time graph heading showing the values in ms. 4. EGW processing time graph heading showing the values in ms.	4	22.3.0

Table 4-45 (Cont.) SEPP 22.4.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34805799	SEPP helm test failing	When the release is deployed with any name other than the ocsepp-release, helm test is failing and not giving the expected output. The code has been updated to remove this dependency and release name has been hardcodedin helm test.	4	22.3.0

Table 4-46 SEPP 22.4.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34533995	RemoteSEPP Delete REST API at config mgr returns success in case underlying failures	Deleting RemoteSEPP REST API at config mgr returns success in case of failure also. RemoteSEPP remains in database even after running delete command. It happens randomly and not for all the cases.	4	22.3.0
34534058	Handshake alert is not getting cleared in some error scenarios	Handshake alert is not getting cleared in some error scenarios: 1. Handshake alert is not getting cleared in some error scenarios. 2. When the handshake failure is due to incorrect plmn. When the handshake failure is due to incorrect plmn.	4	22.3.0
34760961	Alert Information is inconsistent between User Guide and YAML alert file	There are differences in OIDs in the SEPP User Guide and YAML alert file.	3	22.2.3
34747086	Some metrics and KPIs have inconsistencies in the documentation	Inconsistencies in the metrics and KPI information for the SEPP 22.3.1 release.	3	22.3.1
34724085	TH Error is not proper if the value of enabled is not true/false	The PUT /sepp-configuration/v1/topology/feature HTTP/2 REST API was giving JSOB parsing error.	4	22.3.0
34663891	SEPP-COM-DB-ERROR-0005 is not observed in case of DB connection failure	Error COM-DB-ERROR-0005 was not generated in case of DB connection failure.	3	22.3.0

Table 4-46 (Cont.) SEPP 22.4.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34663845	In the CNCC GUI, under Option section status code is displayed intermittently	In CNC Console GUI, under Topology Hiding, on the Option screen status code isdisplayed as 500 intermittently then vanishes. Also, when user opens the edit window status code disappears after a few seconds. Hence, if a user clickson save without making any changes it displays error for missing status code.	4	22.3.0
34657857	No data being displayed for metrics ocsepp_pn32f_outgoing_connections and ocsepp_cn32f_outgoing_connections	Even after a 12 hour run there was no data for metrics,ocsepp_pn32f_outgoing_connections and ocsepp_cn32f_outgoing_connections. Issue is error responses in certain scenarios was not getting updated on code	3	22.3.0
34655474	Multiple caroot concatenation procedure missing in user guide	SEPP document does not contain the details about multiple CA root concatenation procedure. For multiple CA root partners, the SEPP CA certificate should contain the CA information in the particular format. The CAs of the roaming partners should be concatenated in the single file separated by eight hyphens as shown below: CA1 content -------- CA2 content -------- CA3 content{noformat} The SEPP Installation and Upgrade Guide is updated with the above information.	4	22.3.0
34647945	Getting a warning while running helm install for SEPP	Helm install and helm upgrade were giving warnings for PDB deprecated versions. Added the support for allowed PDB versions.	4	22.3.0
34647919	Update custom yaml to make it less error prone	There were some discrepancies found in custom-values.yaml and internal values.yaml file. The custom-values.yaml file should take global input for repository and CNDB.	3	22.3.0

Table 4-46 (Cont.) SEPP 22.4.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34647410	Incorrect error code returned in case user tries to update mandatory parameter in remotesepp config	Instead of error code SEPP-COM-DB-ERROR-0012, error SEPP-COM-DB-ERROR-0010 is observed when user tries to update mandatory parameters (Name or SeppFQDN).	4	22.3.0
34627787	Ambiguity observed in metric names	Names of the following metrics do not clarify the purpose of the metric, that is,if they are related to pn32 or cn32: ocsepp_n32c_handshake_reInitiation_failure ocsepp_n32c_reinit_handshake_failure	4	22.3.0
34598843	Format response for PATCH request in case of failure scenario	Response is not formatted. Formatting was required for displaying of title, status, detail, cause, and invalidParameters in some of the responses that are raised in different scenarios.	4	22.3.0
34598746	Discrepancy observed in display of invalid Parameters	In POST and PUT request for remotesepp, if a user does not mention name/seppfqdn/plmnIdList, invalidParam are not displayed separately. Instead, these parameters are displayed as a part of cause.	4	22.3.0
34597783	Error format not proper if security capability is not TLS/PRINS	When the user creates RemoteSEPP using REST APISet SecurityCapability as "ABC" and run the request, SEPP throws "SON parse error: Cannot deserialize value of type".	4	22.3.0
34589890	Incorrect invalidParam returned as a result of a PATCH request for Remote sepp configuration	In remotesepp config, if isEnabled is set to true and user sends a patchrequest to set it as true, the the invalidParam still is displaying all parameters asnull. only isEnabled set to true should be displayed. PATCH request was failing with 400 error code.	4	22.3.0
34527183	SEPP adding both Server and via header if next hop is down	Added and supported use cases to handle server header and via header configuration in SEPP.	3	22.3.0

Note:

Resolved bugs from 22.3.x have been forward ported to Release 22.4.0.

4.2.13 UDR Resolved Bugs

Table 4-47 UDR 22.4.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35171984	UDR 22.4.0: Unable to Delete the Provisioned Subscriber	The delete subscriber operation was not working when UDR was installed in nudr-dr mode.	2	22.4.0
35073690	UDR provisioning with NetCracker is not working after upgrade to 22.4.0	While upgrading UDR from 22.1.0 to 22.4.0, the UDR provisioning with NetCracker was not working. Ingressgateway was throwing "Internal Server Error".	2	22.4.0

Table 4-48 UDR 22.4.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34866059	Observing DIAMETER_UNABLE_TO_COMPLY in PUA for entity Deletion	DIAMETER_UNABLE_TO_COMPLY in PUA, when PCRF sends profile update request to UDR to delete an Entity present in VSA.	2	22.4.0
34872166	EXPORT_TOOL_STATUS cleans up the latest jobID for every new month	When there is change in the calendar month, the cleanup of older export files is done in the latest month instead of the previous month. If the subscriber export tool feature is run in the previous month, it need to be deployed again before triggering the same feature for the next month.	3	22.4.0
34848933	GET & Delete Behavior is incorrect for UDR Provisioning with IMSI	After Policy Data is created and deleted with only VSA payload, GET and Delete behavior is incorrect for UDR provisioning with IMSI.	3	22.4.0

Table 4-48 (Cont.) UDR 22.4.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34941991	EIR Access Logs Status Should have 0 and 1 for black list and greylist	EIR access logs should have 0 for blacklist and 1 for greylist but in the current EIR access logs, it is 1 for greylist and 2 for blacklist.	3	22.4.0
34933441	"Subscriber Bulk Import Tool for EIR" Doc Issues in UDR User Guide	Subscriber Bulk Import Tool for EIR section in the User Guide is updated with helm install command and supported PDBI commands.	3	22.4.0
34917691	Payload is mentioned for GET request in UDR Rest Api Guide	Payload mentioned for GET request in the Default Entities Supported on 4G UDR using VSA in 4G Policy Data Operations section is deleted.	3	22.4.0

Table 4-49 UDR 22.4.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34716546	Multiple service in PROVGW is having Jaeger error	The config-server service and provgw-config service have jaeger error.	2	22.2.1
34384541	LCI Header format for IGW contains load-metric value with decimal places > 3	Load metric must be upto 3 decimal digits string and the value range must be from 0 to 100.	3	22.2.0
34374953	ProvGw XML structure: End Tag mismatch in between 4G-UDR and 5G-UDR	There is a end tag mismatch between 4G and 5G UDR because the response is not as per 4G UDR output.	3	22.2.0
34647413	Multiple service in SLF is having Jaeger error	The config-server service has Jaeger error.	3	22.2.1
34672462	UDR respond with 400 BAD_REQUEST to cnPCRF PATCH	UDR responds 400 BAD_REQUEST to cnPCRF patch.	3	22.3.1
34647409	SLF/ProvGW HTTP2.remote.resets	HTTP2.remote.resets was observed across the SLF on multiple pods.	3	22.2.1
34744530	DOC: Queries regarding Access Token Validation Provisioning export and description	By default there is no value configured for access token validation for signaling and provisioning.	3	22.3.0

Table 4-49 (Cont.) UDR 22.4.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34647100	DOC: LCI/OCI Header are not provided in the response messages	To provide overload information, SLF should sent LCI and OCI Header to NRF in response to nf-group-id look up.	3	22.2.1
34825825	DOC: Doc Unclear Whether nudr-notify-service Microservice Required For UDR Deployed As EIR	EIR mode does not require the nudr-notify-service.	3	22.3.3
34659941	DOC: SLF Overload Control detail are not in the user guide	SBI overload control feature description and parameter description were required in the User Guide.	4	22.2.1

4.2.14 Common Services Resolved Bugs

4.2.14.1 App-Info Resolved Bugs

Release 22.4.0

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

4.2.14.2 ASM Configuration Resolved Bugs

Release 22.4.0

There are no resolved bugs in this release.

4.2.14.3 ATS Resolved Bugs

ATS Release 22.4.0

There are no resolved bugs in ATS Release 22.4.0.

4.2.14.4 Alternate Route Service Resolved Bugs

Table 4-50 Alternate Route Service 22.4.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
34699921	Weight should be an optional field in Alternate route	The new configuration parameter, `sbiRoutingWeightBasedEnabled`, should be backward compatible and have a default value.	3	22.4.0

4.2.14.5 Debug Tool Resolved Bugs

Release 22.4.0

There are no resolved bugs in this release.

4.2.14.6 Egress Gateway Resolved Bugs

Table 4-51 Egress Gateway 22.4.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
34614513	NRF IGW memory gets exhausted when kafka connection is broken	When kafka connection is broken, the Egress Gateway memory shoots up to the maximum allocated value. This restarts Egress Gateway.	3	22.3.6
34644877	NRF http2.remote.resets	If DNS refresh resulted in a new IP resolution, then existing connection should be shutdown gracefully.	3	22.4.0
34608111	Increase in Memory Consumption observed during traffic run on IGW/EGW with Message copy enabled	Increase in memory consumption was observed during traffic run on Egress Gateway when message copy was enabled.	3	22.4.0

Table 4-51 (Cont.) Egress Gateway 22.4.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
34708664	EGW is sending "502 UPE upstream_reset_before_response_started{protocol_error} Error"	Egress Gateway is sending "502 UPEupstream_reset_before_response_started{protocol_error} Error" when notification retry case is run on ASM setup.	2	22.3.9
34747219	UE-Subscriber-Activity-Logging: SAL is not working	UE-Subscriber-Activity-Logging: SAL is not working for n1_message_notify.	3	22.3.2

4.2.14.7 Helm Test Resolved Bugs

Release 22.4.0

There are no resolved bugs in this release.

4.2.14.8 Ingress Gateway Resolved Bugs

Table 4-52 Ingress Gateway 22.4.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
34614513	NRF IGW memory gets exhausted when kafka connection is broken	When kafka connection is broken, the Ingress Gateway memory shoots up to the maximum allocated value. This restarts Ingress Gateway.	3	22.3.6
34717112	In IGW config-map ConfigurableErrorCodes configured at route level are not considered	Configurable Error Codes configured at route level for XFCC feature are not working as expected.	3	22.4.0

Table 4-52 (Cont.) Ingress Gateway 22.4.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
34608111	Increase in Memory Consumption observed during traffic run on IGW/EGW with Message copy enabled	Increase in memory consumption was observed during traffic run on Ingress Gateway when message copy was enabled.	3	22.4.0
34747219	UE-Subscriber-Activity-Logging: SAL is not working	UE-Subscriber-Activity-Logging: SAL is not working for n1_message_notify.	3	22.3.2
34646754	Istio-proxy not recognizing port name http1-tcp on IGW service	istio-proxy does not recognize or allow the name "http1-tcp".	3	22.1.6
34717112	ConfigurableErrorCodes configured at route level are not working	ConfigurableErrorCodes configured for XFCC feature at route level are not working.	3	22.4.0
34609824	Default error codes profiles	There were inconsistencies between error code profiles and their names. They have been reorganized for consistency.	3	22.3.4
34609888	ExceptionType ERR_124 defined for OAuth Validation is not as expected	The Exception type define under ERR_124 is“OAUTH_PRODUCER_PLMNID_MISMATCH“ instead of“OAUTH_AUDIENCE_NOT_PRESENT_OR_INVALID“.	3	22.3.3

4.2.14.9 Mediation Resolved Bugs

Table 4-53 Mediation 22.4.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34355757	Issue with Mediation Rule: "add(String path, T value)" body rule api & "del(String path, T value)" header and body rule api	Issue with Mediation Rule: "add(String path, T value)" body rule api & "del(String path, T value)" header and body rule api	3	22.2.0
34459393	Mediation microservice is going in CrashLoopBackOff state after setting LOG_LEVEL in deployment file to RULE_TRAIL	Mediation microservice is going in CrashLoopBackOff state after setting LOG_LEVEL to RULE_TRAIL in deployment file.	3	22.2.1
34491723	Mediation trigger point does not work when two rules exist with different httpmethods combinations and one rule is deleted	Mediation trigger point does not work when two rules exist with different http methods combinations and one rule is deleted.	3	22.3.0
34348065	When creating mediation rules, SCP does not report correct error details when header or body condition blocks exceed maximum values	When creating mediation rules, SCP does not report correct error details when header or body condition blocks exceed maximum values.	4	22.2.0
34504199	SCP shows inconsistent error details when a mandatory parameter is missing while creating mediation trigger point	SCP shows inconsistent error details when a mandatory parameter is missing while creating mediation trigger point.	4	22.3.0
34487740	SCP displays the incorrect error detail cause when the start range exceeds the end range while creating mediation trigger rule	SCP displays the incorrect error detail cause when the start range exceeds the end range while creating mediation trigger rule.	4	22.3.0

4.2.14.10 NRF-Client Resolved Bugs

Table 4-54 NRF-Client 22.4.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34767664	Warnings observed while performing Helm Install/Upgrade	Inside nrf-client-nfmanagement/ templates/hooks.yaml. `SERVICE_MESH_CHECK` variable is mentioned twice inside a single block thus giving a warning while running `helm install`command.	4	22.3.1
34836483	Add Resource version to HPA/PDB resources while supporting multiple Versions through helm	Upgrade/Rollback failes due to conflicting in hpa/pdb resources. When different versions of K8s APIs get created with the same name between upgrades, ApiVersion value like "v1" or "v2beta1" was appended to resource's name to make it different in case apiVersion changes.	2	22.3.0
34647881	Add minReplicas and maxReplicas to common services (SLF)	Customer is asking engineering to add the minReplicas and maxReplicas for nfmanagement.	2	22.3.0
34652873	UDR is going to SUSPEND State after one hour of registration	UDR is going to suspended state after 1 hour of registration. The problem is '**envMysqlSecondaryHost**' environment variable is not defined, therefore, it takes the default value of **'database-mysql'** and since that resource is not installed, the error is generated. To fix it the environment variable '**envMysqlSecondaryHost**' now it's not necessary to define.	2	22.3.0

Table 4-54 (Cont.) NRF-Client 22.4.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34596069	Nrf-Client-nfmanagment errors impact 100% call failure on nrf-client-discovery pod	Once the Egress Gateway pod enters a non-response state, NrfClient mgmt pods got some error leg, which impacts Nrfdiscovery pods. This leads to 100% call failure for Nrf discovery requests. i.e. if NrfMgmt pod mis-fires, we'll have 100% failure for discovery requests, which it's considered serious.	2	22.3.2
34645097	PCF NRFClient MGMTPod sending intermittent"http2.remote_reset" even with 200 success response	NRFClient MGMT Pod is sending "http2.remote_reset" intermittently even with 200 responses.	3	22.4.0
34609875	nrf-client-nfdiscovery shows "Healthy NRF Routes available, cannot send Request"	The nrf-client-nfdiscovery pod can not reach Healthy NRF Routes available, so cannot send Request.	3	22.3.0
34836499	"envNfNamespace" variable is impacting single NRF-M pod deployment	NfManagement deployment fails due to "envNfNamespace" variable missing, this happens irrespectively of single or multipod deployment.	3	22.3.0

4.2.14.11 Perf-Info Resolved Bugs

Release 22.4.0

There are no new resolved bugs in this release.

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 Release 22.4.7

There are no known bugs in this release.

> **Note:**
> The known bugs from 22.3.x have been forward ported to Release 22.4.7.

BSF Release 22.4.5

There are no known bugs in this release.

> **Note:**
> The known bugs from 22.3.x have been forward ported to Release 22.4.5.

BSF Release 22.4.2

There are no known bugs in this release.

> **Note:**
> The known bugs from 22.3.x have been forward ported to Release 22.4.2.

BSF Release 22.4.0

There are no known bugs in this release.

> **Note:**
> The known bugs from 22.3.x have been forward ported to Release 22.4.0.

4.3.2 CNC Console Known Bugs

CNC Console Release 22.4.3

There are no known bugs in this release.

CNC Console Release 22.4.2

There are no known bugs in this release.

CNC Console Release 22.4.1

There are no known bugs in this release.

CNC Console Release 22.4.0

There are no known bugs in this release.

4.3.3 DBTier Known Bugs

DBTier 22.4.4 Known Bugs

Table 4-55 cnDBTier 22.4.4 Known Bugs

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

DBTier Release 22.4.3

Table 4-56 DBTier 22.4.3 Known Bugs

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

Table 4-56 (Cont.) DBTier 22.4.3 Known Bugs

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

Table 4-56 (Cont.) DBTier 22.4.3 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35734862	Helm chart takes wrong startNodeId for ndbmysqld from custom values.yaml	Helm chart picks incorrect `startNodeId` value for the `ndbmysqld` pod from the `custom values.yaml` file.	The replication SQL pod reads the node ID that belongs to the APP pod. Therefore, if the APP pod is not present for the specified node, then the `init` container of the replication SQL pod doesn't come up. **Workaround**: Before installing or upgrading DBTier, perfrom the following steps to update the `sts.yaml` file: 1. Open the `sts.yaml` file in the `occndbtier/charts/api/templates/` folder. 2. Update the configuration in line number "471" from `value: {{ .Values.global.ndbapp.startNodeId | default 70 | quote }}` to `value: {{ .Values.global.api.startNodeId | default 56 | quote }} .`	3	23.1.2

DBTier Release 22.4.2

Table 4-57 DBTier 22.4.2 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35848919	Connectivity fails towards "running" ndbappmysqld pods' mysql-server during upgrade. Behaviour not seen during pod termination.	ndbappmysqld pods move to the running status before the mysql process is ready.	During a rolling restart of ndbappmysqld pods, two ndbappmysqld pods may not get connected to the NF application through the connectivity service at the same time leading to potential traffic loss. **Workaround**: Configure more than two ndbappmysqld pods while performing a rolling restart of ndbappmysqld pods to ensure that there are operational pods to manage the incoming traffic.	2	23.3.0
35734862	Helm chart takes wrong startNodeId for ndbmysqld from custom values.yaml	Helm chart picks incorrect `startNodeId` value for the `ndbmysqld` pod from the `custom values.yaml` file.	The replication SQL pod reads the node ID that belongs to the APP pod. Therefore, if the APP pod is not present for the specified node, then the `init` container of the replication SQL pod doesn't come up. **Workaround**: Before installing or upgrading DBTier, perfrom the following steps to update the `sts.yaml` file: 1. Open the `sts.yaml` file in the `occndbtier/charts/api/templates/` folder. 2. Update the configuration in line number "460" from `value: {{ .Values.global.ndbapp.startNodeId | default 70 | quote }}` to `value: {{ .Values.global.api.startNodeId | default 56 | quote }}` .	3	23.1.2

DBTier Release 22.4.1

Table 4-58 cnDBTier 22.4.1 Known Bugs

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

DBTier Release 22.4.0

Table 4-59 cnDBTier 22.4.0 Known Bugs

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

4.3.4 CDCS Known Bugs

CDCS Release 22.4.2

There are no known bugs in CDCS Release 22.4.2.

CDCS Release 22.4.1

There are no known bugs in CDCS Release 22.4.1.

CDCS Release 22.4.0

There are no known bugs in CDCS Release 22.4.0.

4.3.5 CNC Policy Known Bugs

CNC Policy 22.4.7 Known Bugs

There are no new known bugs in this release.

> **Note:**
>
> The known bugs from 22.3.x have been forward ported to Release 22.4.7.

CNC Policy 22.4.6 Known Bugs

There are no new known bugs in this release.

> **Note:**
>
> The known bugs from 22.3.x have been forward ported to Release 22.4.6.

Table 4-60 CNC Policy 22.4.5 Known Bugs

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

Table 4-61 CNC Policy 22.4.4 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 metric in case of response failure is being reported twice compared to the actual value.	The number of failure response metrics for LDAP call flow will be twice the 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

> **Note:**
>
> The known bugs from 22.3.x have been forward ported to Release 22.4.4.

CNC Policy 22.4.3 Known Bugs

There are no new known bugs in this release.

> **Note:**
>
> The known bugs from 22.3.x have been forward ported to Release 22.4.3.

CNC Policy 22.4.2 Known Bugs

There are no new known bugs in this release.

> **Note:**
>
> The known bugs from 22.3.x have been forward ported to Release 22.4.2.

Table 4-62 CNC Policy 22.4.1 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
34964990	UE Policy Message Size shall support bigger range.	The range for the N1 message and manage UE Policy section maximum size from 0 to 9000 Bytes is not supported. This range should be fixed, or else operators will not be able to put bigger values for the range and messages will get unnecessarily fragmented.	The customer cannot fit a manage UE policy command (N1) message larger than 9000 bytes in a single fragment. The system will automatically fragment the message into multiple manage UE policy command messages. **Workaround**: None	3	22.4.0

Note:

The known bugs from 22.3.x have been forward ported to Release 22.4.1.

Table 4-63 CNC Policy 22.4.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
34811446	IP Can Session Termination Blockly Not working	Policy Action "Release all PCEF/TDF sessionassociated with IP-CAN Session" fails when the Rx session is with complete /128 bit IPv6 address and Gx session to which it binds to is /64 bit IPv6 prefix. This is because a direct comparison of the IPv6 address from Rx and IPv6 prefix in Gx session is being done.	Policy Action "Release all PCEF/TDF sessionassociated with IP-CAN Session" fails when the Rx session is with complete /128 bit IPv6 address and Gx session to which it binds to is /64 bit IPv6 prefix. This is because a direct comparison of the IPv6 address from Rx and IPv6 prefix in Gx session is being done. **Workaround**: Either use IPv4 address or avoid using this blockly when Gx is IPv6/64 bit prefix and Rx is complete/128 bit prefix.	3	22.2.0

> **Note:**
>
> The known bugs from 22.3.1 and 22.3.2 have been forward ported to Release 22.4.0

4.3.6 CNE Known Bugs

CNE 22.4.5 Known Bugs

There are no new known bugs in this release. For existing known bugs, see CNE 22.4.3 Known Bugs.

CNE 22.4.4 Known Bugs

There are no new known bugs in this release. For existing known bugs, see CNE 22.4.3 Known Bugs.

Table 4-64 CNE 22.4.3 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35182156	LBVMs unable to communicate with backend services	Load Balancer Virtual Machines (LBVM) are unable to communicate with the backend services as the *k8s* Security Group (SG) overrides the *k8s_node_secgroup* SG. To overcome this issue, both the *k8s* and *k8s_node_secgroup* SGs, that are applied to worker nodes, must be combined.	When there are two SGs that are used in the same node, one SG overrides the other SG as per the rules applied. Therefore, the rules go missing and node communication does not work. **Workaround**: Manually add the rules needed at the openstack desktop.	2	22.4.1

Table 4-64 (Cont.) CNE 22.4.3 Known Bugs

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

Table 4-65 CNE 22.4.2 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
34978552	After Upgrade to 22.3 VMware LBs are left with dysfunctional ifcfg file	After CNE upgrade on VMware cluster, most of the STANDBY LBs and several ACTIVE LBs are left with a dysfunctional /etc/sysconfig/networking-scripts/ifcfg-ens192 file.	After an upgrade, during a Load Balancer VM (LBVM) switchover, the current VMware version requires vms to reboot to remove the active interfaces and make the new ones active. This behavior leads to several interfaces, that were supposed to be deleted from configuration file, to remain active leaving the cluster in a failed state. **Workaround**: Manually configure LBVM configuration files to point to the correct interfaces.	2	22.4.0

Table 4-65 (Cont.) CNE 22.4.2 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35182156	LBVMs unable to communicate with backend services	Load Balancer Virtual Machines (LBVM) are unable to communicate with the backend services as the *k8s* Security Group (SG) overrides the *k8s_node_secgroup* SG. To overcome this issue, both the *k8s* and *k8s_node_secgroup* SGs, that are applied to worker nodes, must be combined.	When there are two SGs that are used in the same node, one SG overrides the other SG as per the rules applied. Therefore, the rules go missing and node communication does not work. **Workaround**: Manually add the rules needed at the openstack desktop.	2	22.4.1

Table 4-66 CNE 22.4.1 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
34984839	Interpod communication not working after applying Egress NAT annotations.	SCP Interpod communication doesn't work after applying Egress NAT annotations `oracle.com.cnc/egress-network: "sig2`. **Workaround**: Install CNE 22.4.1.0.1 patch from MOS.	Application functionality fails on CNE 22.4.0.	2	22.4.0

Table 4-66 (Cont.) CNE 22.4.1 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35016981	DBTier geo-replication flow in vCNE requires egress traffic on TCP ports 2022 and 3306 in LBVMs. Openstack security group is missing the egress rules to allow this flow.	LBVMs must be configured to allow TCP ingress and egress traffic on ports 2022 and 3306. The Openstack security group doesn't have the egress rules to allow the ports. **Workaround:** • For manual configuration of these ports, log in to Openstack and select **Security Groups** under **Network**. • For the corresponding cluster, search for the following groups: MBIPs Egress NAT Security Group, MBIPs Security Group, and default group. • For each group, click **Manage rules**. • Add rule for each port (2022 and 3306) in the egress direction.	cnDBTier georeplication doesn't not work.	2	22.4.0

CNE 22.4.0 Known Bugs

There are no known bugs in this release.

4.3.7 NEF Known Bugs

OCNEF Release 22.4.4

There are no known bugs in this release.

OCNEF Release 22.4.3

There are no known bugs in this release.

OCNEF Release 22.4.2

There are no known bugs in this release.

OCNEF Release 22.4.1

There are no known bugs in this release.

OCNEF Release 22.4.0

There are no known bugs in this release.

4.3.8 NRF Known Bugs

NRF 22.4.4 Known Bugs

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

NRF 22.4.3 Known Bugs

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

Table 4-67 NRF 22.4.2 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
34986707	ocnrf_replication_status_check_total does not get scraped from the artisan pod	ocnrf_replication_status_check_total metric is not pegged for the artisan pod.	OcnrfReplicationStatusMonitoringInactive alert will be raised for the pod. Update the alert expression to exclude nrfartisan service like below: sum by(pod) (irate(ocnrf_replication_status_check_total{container!~"nrfauditor|nrfartisan" }[5m])) == 0	3	22.3.2

Table 4-68 NRF 22.4.1 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
34844121	NRF Auditor: Install hook and auditor service are taking leaderElectionDbName from different places	NRF auditor leader: Install hook and auditor service are taking leaderElectionDbName from different places. Hooks area which is install is taking leaderElectionDbName from secret but Auditor business logic is taking db name from values.yaml	While configuring secrets leaderElectionDbName value shall match with global.database.leaderElectionDbName in custom values.yaml, otherwise Auditor microservice will not come up. **Workaround**: Note is added in OCNRF installation guide to match the leaderElectionDbName value in secret with global.database.leaderElectionDbName in custom values.yaml file used for deployment.	3	22.3.1

Table 4-68 (Cont.) NRF 22.4.1 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
34986707	ocnrf_replication_status_check_total does not get scraped from the artisan pod	ocnrf_replication_status_check_total metric is not pegged for the artisan pod.	OcnrfReplicationStatusMonitoringInactive alert will be raised for the pod. Update the alert expression to exclude nrfartisan service like below: sum by(pod)(irate(ocnrf_replication_status_check_total{container!~"nrfauditor|nrfartisan" }[5m])) == 0	3	22.3.2

Table 4-69 NRF 22.4.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
34844121	NRF Auditor: Install hook and auditor service are taking leaderElectionDbName from different places	NRF auditor leader: Install hook and auditor service are taking leaderElectionDbName from different places. Hooks area which is install taking leaderElectionDbName from secret but Auditor business logic is taking db name from values.yaml	While configuring secrets leaderElectionDbName value shall match with global.database.leaderElectionDbName in custom values.yaml otherwise Auditor microservice will not come up. **Workaround**: Note is added in OCNRF installation guide to match the leaderElectionDbName value in secret with global.database.leaderElectionDbName in custom values.yaml file used for deployment.	3	22.3.1

Table 4-69 (Cont.) NRF 22.4.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
34848377	NRF Configuration Microservice issues when connectivity between NRF and DB is down	NRF Configuration Microservice issues when connectivity between NRF and DB is down.	When POD is in Running Status, when connectivity with DB goes down then, Configuration Service (its goes in non ready then restarts, then startup probe fails then keeps restarting). **Workaround**: No workaround but when DB connectivity with OCNRF gets restored, then Configuration microservice becomes ready and is stable).	3	22.4.0

Table 4-69 (Cont.) NRF 22.4.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
34848384	NRF Auditor Microservice issues when connectivity between NRF and DB is down	NRF Auditor Microservice issues when connectivity between NRF and DB is down.	When POD is in Running Status, when connectivity with DB goes down then Auditor -- It's in not ready state (as expected). **Workaround**: No workaround but when connectivity gets restored, Auditor (it restarts once, then becomes ready and is stable).	3	22.4.0

4.3.9 NSSF Known Bugs

Table 4-70 NSSF 22.4.4 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35035379	while adding the Amf-set in CNCC UI, OCNSSF send multiple unknown Headers in discovery message request to NRF	Based on the operator configuration, NSSF sends an on-demand Discovery and Subscription to NRF. The issue is in PCAP logs and many unknown headers are being seen. The message is fine till it reaches Egress Gateway (EGW) but the messages that come out of EGW are having these headers.	No impact on service as NRF is processing the message and subscriptions are successful. **Workaround**: The issue is not being reproduced in dev setups but is being observed in one of the SPAD setups.	3	22.4.2
35201056	NSSF Egress gateway service is not present in the Jaeger GUI	The Egress Gateway service is not available in the Jaeger GUI even though Jaeger tracking is enabled in NSSF custom value.yaml and Ingress & Egress Gateway.	No impact on service as there is no packet loss, Unable to check Jaeger logs. **Workaround**: No workaround available	3	22.3.2

Table 4-70 (Cont.) NSSF 22.4.4 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35261720	NSSF - namespace name is hardcoded in the nssf-alert-rules.yaml	The namespace name is hard-coded in the *nssf-alert-rules.yaml*. There are multiple entries of the hard-coded namespace value “*ocnssf*”, and each needs to be edited before deployment in any environment.	No impact on service. The operator has to update (replace) ocnssf with the namespace where the deployment exists. **Workaround**: No workaround available	3	22.4.3

Table 4-71 NSSF 22.4.2 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
34898985	ATS Version in ATS GUI is wrong	The ATS version in GUI is wrong.	OCNSSF version in CNC GUI is coming as 22.4.0 for NSSF 22.4.1 **Workaround:** There is a workaround to update the version in Admin GUI.	3	22.4.1

Table 4-71 (Cont.) NSSF 22.4.2 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
34939923	ocnssf-nssubscription service pod is not coming up while doing upgradation from Version 22.3.1 to 22.4.1	Intermittently when DB data for event_trigger_subscription_map table contains hanging foreign keys, and at that time action of NSSF upgrade occurs. This makes the NsSubscription por restart continuously.	The issue occurs only in case of an upgrade when transient data is present. **Workaround:** Make sure event_trigger_subscription_map is empty before upgrading, hence no pending notifications. Post upgrade, remove the transient content.	3	22.4.1

NSSF 22.4.1 Known Bugs

There are no new known bugs in this release. For existing known bugs, see Table 4-72.

Table 4-72 NSSF 22.4.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
34784403	NSSF is not able to handle a discovery response which contains AMF profile not supporting tac ranges.	AMF profile is configured with tacRangeList with NRF, but the NSSF selection request is not successfully returning the candidateAmfList. However, when we remove the tacRangeList and register with NRF, then the NSSF selection request successfully returns the candidateAmfList.	The impact is in the situations when AMF Profile has a TAI Range configured and Feature to resolve candidate is enabled as true, NSSF will not consider those AMFs as candidate AMFs. **Workaround**: NA	3	22.3.0

Table 4-72 (Cont.) NSSF 22.4.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
34797626	Unable to remove configuration content created by Auto-Population of Configuration Based on NsAvailability	NsAvailability update PUT from AMF creates configuration at NSSF in case when the content is not previously configured by the Operator. NsAvailability update delete from AMF must delete the content in case no other AMF is bound with that Data, intermittantly when delete call is being run the call is getting responded with 500 Error from NSSF.	Intermitanty NsAvailability Delete is failing, AMF shall trigger a retransmission of the NsAvailability Delete request. **Workaround**: NA	3	22.3.0

4.3.10 NWDAF Known Bugs

NWDAF 22.1.0 Known Bugs

There are no known bugs.

4.3.11 SCP Known Bugs

SCP 22.4.4 Known Bugs

There are no new known bugs in this release. For existing known bugs, see Table 4-73.

SCP 22.4.3 Known Bugs

There are no new known bugs in this release. For existing known bugs, see Table 4-73.

SCP 22.4.2 Known Bugs

There are no new known bugs in this release. For existing known bugs, see Table 4-73.

SCP 22.4.1 Known Bugs

There are no new known bugs in this release. For existing known bugs, see Table 4-73.

Table 4-73 SCP 22.4.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
34838348	Intermittent errors observed with model D Traffic with enforceReqSpecificSvcDiscovery set to false.	Internittent 5xx errors are observed when Model D performance traffic was run with 66 profiles discovery from NRF and enforceReqSpecificSvcDiscovery is set to false.	Very few requests routing failures and errors might be observed for Model D traffic. **Workaround**: Set the enforceReqSpecificSvcDiscovery parameter to true to reduce the size of discovery response received from NRF for 66 profiles for Model D traffic.	3	22.4.0
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 testcases are removed. **Workaround**: Comment out ATS cases failing due to ASM issue.	4	22.1.0

4.3.12 SEPP Known Bugs

SEPP Release 22.4.4

There are no new known bugs in this release. For existing known bugs, see SEPP Release 22.4.3 Known Bugs and SEPP Release 22.4.1 Known Bugs.

Table 4-74 SEPP Release 22.4.3 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
35036599	Total traffic loss after upgrade when global Ingress rate limiting feature is enabled	There is total traffic failure when SEPP is upgraded from 22.3.x and 224.x to 23.1.0 and rate limit feature is ON. The below exception is observed after the upgrade and the traffic is fine if Ingress pod is restarted. Role=SpringframeworkBootLoaderJarLauncher)) io.github.bucket4j.BucketConfiguration; class invalid for deserialization", "message":"(Wrapped: Failed request execution for MapDistCache service on Member(Id=2)	If global Rate Limiting feature is enabled, traffic is in progress and upgrade is performed to 22.4.x or 23.1.0 release. After the upgrade, n32-ingress-gateway will stop processing the traffic, and there will be total traffic loss. **Workaround**: The following workarounds can be used: 1. If SBI traffic is in progress during the upgrade, restart the n32-ingress-gateway after the upgrade. System will recove	2	22.4.0

Table 4-74 (Cont.) SEPP Release 22.4.3 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
			r and start processing the traffic. 2. Perform an upgrade with Global Rate Limiting feature disabled. 3. Perform the upgrade to 22.4.3 without traffic.		

For existing known bugs, see, Table 4-75

SEPP Release 22.4.2 Known Bugs

There are no new known bugs in this release. For existing known bugs, see Table 4-75.

Table 4-75 SEPP Release 22.4.1 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
34627763	pn32f_jetty, cn32f_jetty, pn32f_server_latency and cn32f_server_latency metrics are not being pegged	Some of the jetty metrics mentioned in the document are not getting pegged.	No impact These metrics are helpful in debugging performance related issues in the network. **Workaround:** There is no workaround. These metrics are mostly used in debugging performance related issues.	3	22.3.0

Table 4-75 (Cont.) SEPP Release 22.4.1 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
34569424	Proper error-reason should be thrown by csepp when n32-ingress service is scaled down at psepp and an interplmn request is sent from csepp to psepp	This scenario is observed when Egress Gateway is not able to send the SBI message to the next node or NF when the NF is unreachable. • HTTP error status in response received by gateway and details can be configured through values.yaml file • Code exception mentioned in error-reason is coming from Egress Gateway code error-reason: org.springframework.web.reactive.function.client.WebClientRequestException:nested exception is java.nio.channels.ClosedChannelException	User will not be able to identify the reason of failure from error cause. **Workaround:** Run kubectl command to verify that all the services are up and running. Wait for the service to come up and issue will get resolved.	3	22.2.0

Table 4-75 (Cont.) SEPP Release 22.4.1 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
34374452	SEPP-COM-xx-ERROR-0103 not observed when n32c pods have been scaled down	On scaling down the pn32c and cn32c pods, if a delete request is processed for the configured remotesepp , 204 is returned. However, the entry is not deleted. And, no error is displayed when POST request is processed if the pods are scaled down.	No impact Run the delete command when all the pods and services are up and running. **Workaround:** Make the pod and service up. Run the command and it will be done successfully.	4	22.3.0
34664359	SEPP micro services traces are not correlated in Jaeger UI	In previous versions when querying traces on JAEGER UI, one single trace was returned with multiple spans from different microservices involved for a single transaction, for example: plmn-ingress-gateway span + cn32f span + n32-egress-gateway span. In 22.3 this correlation is not happening anymore and every microservice is generating a different trace.	No functional impact Correlation was helpful to quickly understand the internal flow of thetransaction and find in which particular microservice a potential problem washappening. **Workaround:** Logs on kibana can be used to check correlation of messages.	3	22.3.0

Table 4-75 (Cont.) SEPP Release 22.4.1 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
34760842	RH SEPP doesn't set a proper authorities in established N32 context with 3GppSbiTargetApiRoot Supported" set to false	RH SEPP attempts to establish N32 context with Remote SEPP 1 and Remote SEPP 2. The following scenarios occur: • Remote SEPP 1 - n32c handshake request with "3GppSbiTargetApiRoot Supported" set to true in the http body. • Remote SEPP 2 - n32c handshake request with "3GppSbiTargetApiRoot Supported" set to false in the http body. RH SEPP handshake status reflects that the established N32 context withRemote SEPP 2 has 3GPP SBI Target API Root Header set to false. The outgoing request from RH SEPP to Remote SEPP 2 has no 3gpp-sbi-target-apiroot but the authority is	When both the consumer and producer SEPPs are Oracle SEPP, the issue will not be observed. Issue will be observed when one of the SEPP is non-Oracle SEPP. **Workaround:** Send a message with 3gpp-sbi-target-api-root header and *3GppSbiTargetApiRootSupported* to be set to true in HELM.	3	22.3.0

Table 4-75 (Cont.) SEPP Release 22.4.1 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
		replaced by the Remote SEPP 2 SEPP identity. This behaviour is incorrect and RH SEPP should set 'authority' header using the value from 3gpp-sbi-target-apiroot header from the incoming request.			

Table 4-76 OCSEPP Release 22.4.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
34498601	N32 IGW dropping traffic silently due to io.netty.util.IllegalReferenceCountException	All Inter PLMN traffic is silently getting dropped at N32 Ingress Gateway when the traffic is run for long duration due to the following error *io.netty.util.IllegalReferenceCountException* on netty threads. Issue is observed after sending traffic for 12 hours at 800 TPS. TPS: 800 TPS Length of run: 12 hours N32 EGW: N32 IGW	SEPP performance runs done for long duration are impacted. Some packets are getting dropped at IGW in lab setup, but in customer deployment, the failed request will be retried on a different SEPP. **Workaround:** The impact of this issue is low. Also, it is an intermittent issue.	3	22.2.0

Table 4-76 (Cont.) OCSEPP Release 22.4.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
34692921	Discrepancy in response if the error response is received from primary SEPP	There is a discrepancy in response received by Gateway when the same error scenario is run on Primary Remote SEPP and Secondary Remote SEPP. In secondary remote SEPP, errors are getting overwritten.	No impact The Error response received by originating NF will be different for the same scenario occurs at primary SEPP or at Secondary SEPP. **Workaround:** Set the desired error response in n32-egress-gateway HELM chart. By doing this, all the remote SEPP sends same error cause to originating NF in the same scenario.	3	22.3.0
34627763	pn32f_jetty, cn32f_jetty, pn32f_server_latency and cn32f_server_latency metrics are not being pegged	Some of the jetty metrics mentioned in the document are not getting pegged.	No impact These metrics are helpful in debugging performance related issues that occur in the network. **Workaround:** There is no workaround.	3	22.3.0

Table 4-76 (Cont.) OCSEPP Release 22.4.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
34569424	Proper error-reason should be thrown by csepp when n32-ingress service is scaled down at psepp and an interplmn request is sent from csepp to psepp	The scenario is observed when Egress Gateway is not able to send the SBI messageto next node/NF when the NF is unreachable. • HTTP error status and details can be configured through values.yaml file • Code exception mentioned in error reason is coming from Egress Gateway code error reason: *org.springframework.web.reactive.function.client.WebClientRequestException* isnested with *java.nio.channels.ClosedChannelException*	User cannot be able to identify the reason of failure from error cause. They have to check the grafana and metrics to find the root cause. **Workaround:** Run kubectl command to verify that all the services are up and running. Wait for the service to come up and issue will get resolved.	3	22.2.0
34374452	SEPP-COM-xx-ERROR-0103 not observed when n32c pods have been scaled down	On scaling down pn32c and cn32c pods, if a delete request is run forconfigured remotesepp, 204 is returned but entry is not deleted.Also, no error is displayed when POST request is run when the pods arescaled down.	No impact. **Workaround:** Run the delete command when all the pods and services are up and running.	4	22.3.0

Table 4-76 (Cont.) OCSEPP Release 22.4.0 Known Bugs

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

Table 4-76 (Cont.) OCSEPP Release 22.4.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
34760842	Remote Host (RH) SEPP doesn't set proper authorities in established N32 context with 3GppSbiTargetApiRootSupported" set to false	RH SEPP attempts to establish N32 context with Remote SEPP 1 and Remote SEPP 2. The following scenarios occur: • Remote SEPP 1 - n32c handshake request with "3GppSbiTargetApiRootSupported" set to true in the http body. • Remote SEPP 2 - n32c handshake request with "3GppSbiTargetApiRootSupported" set to false in the http body. RH SEPP handshake status reflects that the established N32 context withRemote SEPP 2 has 3GPP SBI Target API Root Header set to false.The outgoing request from RH SEPP to Remote SEPP 2 has no 3gpp-sbi-target-apiroot but the authority is replaced by the Remote SEPP 2 SEPP identity. RH SEPP should set as authority the identity found	When both the consumer and producer SEPPs are Oracle SEPP, the issue will not be observed. Issue will be observed when one of the SEPP is non-Oracle SEPP. **Workaround:** Send a message with 3gpp-sbi-target-api-root header and set the parameter, 3GppSbiTargetApiRootSupported, to True in HELM.	3	22.3.0

Table 4-76 (Cont.) OCSEPP Release 22.4.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
		in the3gpp-sbi-target-apiroot from the incoming request.			
34374437	SEPP is unable to register to NRF when NRF re-installed	SEPP is unable to register to NRF when NRF re-installed. Example: SEPP22.2.0 and NRF 22.1.2 are up and running. SEPP isregistered with NRF. NRF is re-installed to 22.2.0. Here SEPP registration fails.	When NRF is reinstalled, SEPP does not automatically register with NRF that results in loss of SEPP registration with NRF. **Workaround:** Restart the plmn-egress gateway. The registration of SEPP to the NRF will be successful.	3	22.3.0

4.3.13 UDR Known Bugs

UDR 22.4.2 Known Bugs

There are no new known bugs in this release. The known bugs from 22.4.x have been forward ported to Release 22.4.2

UDR 22.4.1 Known Bugs

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

Table 4-77 UDR 22.4.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
34835495	perf-info is throwing error if there are no spans present in jaeger query service	When no traces are found in jaeger query service, per-info service logs have jaeger error.	This is non-service impacting and only logs error when no spans are available. **Workaround** There is no workaround.	3	22.4.0

Table 4-77 (Cont.) UDR 22.4.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
34872166	EXPORT_TOOL_STATUS cleans up the latest jobID for every new month	When the subscriber export tool is scheduled with daily runs and when there is change in the calendar month, the cleanup of older export files is done in the latest month instead of the previous month files.	If the subscriber export tool feature is run in the previous month, it needs to be deployed again before triggering the same feature for the next month. A note is added in the Running SLF-NewFeatures Pipeline section in the *Oracle Communications Cloud Native Core Automated Testing Suite Guide*. **Workaround** Re-install the subscriber export tool or execute kubectl delete pod.	3	22.4.0

4.3.14 Common Services Known Bugs

4.3.14.1 Alternate Route Service Known Bugs

Release 22.4.0

There are no new known bugs in this release.

4.3.14.2 ASM Configuration Known Bugs

Release 22.4.0

There are no known bugs in this release.

4.3.14.3 ATS Known Bugs

Release 22.4.0

There are no new known bugs in this release.

4.3.14.4 App-Info Known Bugs

Release 22.4.0
There are no known bugs in this release.

4.3.14.5 Debug Tool Known Bugs

Release 22.4.0

There are no known bugs in this release.

4.3.14.6 Egress Gateway Known Bugs

Egress Gateway 22.4.0 Known Bugs

There are no new known bugs in this release.

4.3.14.7 Helm Test Known Bugs

Release 22.4.0

There are no known bugs in this release.

4.3.14.8 Ingress Gateway Known Bugs

Ingress Gateway 22.4.0 Known Bugs

There are no new known bugs in this release.

4.3.14.9 Mediation Known Bugs

Release 22.4.0

There are no new known bugs in this release.

4.3.14.10 NRF-Client Known Bugs

Release 22.4.0

There are no new known bugs in this release.

4.3.14.11 Perf-Info Known Bugs

Release 22.4.0

There are no new known bugs in this release.