Oracle® Communications

Cloud Native Core Release Notes

Release 3.24.2

G11304-42

June 2025

Oracle Communications Cloud Native Core Release Notes, Release 3.24.2

G11304-42

Contents

1 Introduction

2 Feature Descriptions

3 Media and Documentation

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 3.24.2 - G11304-42, June 2025

UDR 24.2.5 Release

Updated the following sections with the details of UDR release 24.2.5:

- Media Pack
- Compatibility Matrix
- UDR Resolved Bugs

Release 3.24.2 - G11304-41, June 2025

Policy 24.2.6 Release

Updated the following section with the details of Policy release 24.2.6:

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

Release 3.24.2 - G11304-40, May 2025

Policy 24.2.1 Release
Updated the description of 36938337 bug in Policy Resolved Bugs section.

Release 3.24.2 - G11304-39, May 2025

cnDBTier 24.2.5 Release
Updated the following sections with the details of cnDBTier release 24.2.5:

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

Release 3.24.2 - G11304-38, May 2025

CNE 24.2.6 Release

Updated the following sections with the details of CNE release 24.2.6:

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

Release 3.24.2 - G11304-37, April 2025

BSF 24.2.3 Release

Updated the following sections with the details of BSF release 24.2.3:

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

Policy 24.2.5 Release

Updated the following section with the details of Policy release 24.2.5:

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

Release 3.24.2 - G11304-36, April 2025

CNC Console 24.2.4 Release

Updated the following sections with the details of CNC Console release 24.2.4:

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

UDR 24.2.4 Release

Updated the following sections with the details of UDR release 24.2.4:

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

Release 3.24.2 - G11304-35, April 2025

SCP 24.2.4 Release

Updated the following sections with the details of SCP release 24.2.4:

- Media Pack
- Compatibility Matrix

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

SEPP 24.2.4 Release

Updated the following sections with the details of SEPP release 24.2.4:

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

Release 3.24.2 - G11304-34, April 2025

NRF 24.2.4 Release

Updated the following sections with the details of NRF release 24.2.4:

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

Release 3.24.2 - G11304-33, April 2025

CNC Console 24.2.3 Release

Updated the following sections with the details of CNC Console release 24.2.3:

- CNC Console Resolved Bugs

OCCM 24.2.3 Release

Updated the following sections with the details of OCCM release 24.2.3:

- OCCM Resolved Bugs

Release 3.24.2 - G11304-32, April 2025

CNC Console 24.2.3 Release

Updated the following sections with the details of CNC Console release 24.2.3:

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

OCCM 24.2.3 Release

Updated the following sections with the details of OCCM release 24.2.3:

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

Release 3.24.2 - G11304-31, April 2025

cnDBTier 24.2.4 Release

Added a known bug, 37761092, in the section cnDBTier Known Bugs for cnDBTier release 24.2.4.

Release 3.24.2 - G11304-30, March 2025

Policy 24.2.4 Release

Updated the following section with the details of Policy release 24.2.4:

- Compatibility Matrix
- Policy Resolved Bugs

Release 3.24.2 - G11304-29, March 2025

Policy 24.2.4 Release

Updated the following section with the details of Policy release 24.2.4:

- Compatibility Matrix

Release 3.24.2 - G11304-28, March 2025

Policy 24.2.4 Release

Updated the following sections with the details of Policy release 24.2.4:

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

Release 3.24.2 - G11304-27, February 2025

cnDBTier 24.2.4 Release

Updated the following sections with the details of cnDBTier release 24.2.4:

- Media Pack
- Compatibility Matrix
- cnDBTier Resolved Bugs

- cnDBTier Known Bugs

OSO 24.2.5 Release

Updated the following sections with the details of OSO release 24.2.5:

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

Release 3.24.2 - G11304-26, February 2025

SCP 24.2.3 Release

Updated the following sections with the details of SCP release 24.2.3:

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

Release 3.24.2 - G11304-25, January 2025

BSF 24.2.2 Release

Updated the following sections with the details of BSF release 24.2.2:

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

Policy 24.2.3 Release

Updated the following sections with the details of Policy release 24.2.3:

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

CNE 24.2.4 Release

Updated the following sections with the details of CNE release 24.2.4:

- Media Pack
- Compatibility Matrix
- CNE Resolved Bugs

Release 3.24.2 - G11304-24, January 2025

cnDBTier 24.2.3 Release

Updated the following sections with the details of cnDBTier release 24.2.3:

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

NRF 24.2.3 Release

Updated the following sections with the details of NRF release 24.2.3:

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

UDR 24.2.3 Release

Updated the following sections with the details of UDR release 24.2.3:

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

Release 3.24.2 - G11304-23, January 2025

CNC Console 24.2.2 Release

Updated the following sections with the details of CNC Console release 24.2.2:

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

SEPP 24.2.3 Release

Updated the following sections with the details of SEPP release 24.2.3:

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

- SEPP Resolved Bugs

Release 3.24.2 - G11304-22, January 2025

OCCM 24.2.2 Release

Updated the following sections with the details of OCCM release 24.2.2:

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

Release 3.24.2 - G11304-21, January 2025

SEPP 24.2.2 Release

Updated the following sections with the details of SEPP release 24.2.2:

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

Release 3.24.2 - G11304-20, December 2024

UDR 24.2.2 Release

Updated the following sections with the details of UDR release 24.2.2:

- Unified Data Repository (UDR)
- UDR Resolved Bugs

Release 3.24.2 - G11304-19, November 2024

cnDBTier 24.2.1 Release

Updated the resolved bugs for 24.2.1 in the cnDBTier Resolved Bugs section.

Release 3.24.2 - G11304-18, November 2024

CNE 24.2.3 Release

Updated the following sections with the details of CNE release 24.2.3:

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

Release 3.24.2 - G11304-17, November 2024

Policy 24.2.2 Release

Updated the following sections with the details of Policy release 24.2.2:

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

Release 3.24.2 - G11304-16, October 2024

SCP 24.2.2 Release

Updated the following sections with the details of SCP release 24.2.2:

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

UDR 24.2.1 Release

Updated the following sections with the details of UDR release 24.2.1:

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

CNE 24.2.2 Release

Updated the following sections with the details of CNE release 24.2.2:

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

NSSF 24.2.1 Release

Updated the following sections with the details of NSSF release 24.2.1:

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

- NSSF Known Bugs

Release 3.24.2 - G11304-15, October 2024

Console 24.2.1 Release

Updated the following sections with the details of Console release 24.2.1:

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

SEPP 24.2.1 Release

Updated the following sections with the details of SEPP release 24.2.1:

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

NRF 24.2.2 Release

Updated the following sections with the details of NRF release 24.2.2:

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

Release 3.24.2 - G11304-14, October 2024

cnDBTier 24.2.2 Release

Updated the following sections with the details of cnDBTier release 24.2.2:

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

Release 3.24.2 - G11304-13, October 2024

CNE 24.2.1 Release

Updated the following sections with the details of CNE release 24.2.1:

- Cloud Native Environment (CNE)
- Media Pack

- Compatibility Matrix
- CNE Resolved Bugs
- CNE Known Bugs

OCCM 24.2.1 Release

Updated the following sections with the details of OCCM release 24.2.1:

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

Release 3.24.2 - G11304-12, October 2024

Policy 24.2.1 Release

Updated the following sections with the details of Policy release 24.2.1:

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

OCI Adaptor 24.2.1 Release

Updated the following sections with the details of OCI Adaptor release 24.2.1:

- OCI Adaptor
- Media Pack
- Compatibility Matrix
- OCI Adaptor Resolved Bugs

Release 3.24.2 - G11304-11, October 2024

BSF 24.2.1 Release

Updated the following sections with the details of BSF release 24.2.1:

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

Release 3.24.2 - G11304-10, September 2024

cnDBTier 24.2.1 Release

Updated the following sections with the details of cnDBTier release 24.2.1:

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

Release 3.24.2 - G11304-09, September 2024

NRF 24.2.1 Release

Updated the following sections with the details of NRF release 24.2.1:

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

SCP 24.2.1 Release

Updated the following sections with the details of SCP release 24.2.1:

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

Release 3.24.2 - G11304-08, August 2024

cnDBTier 24.2.0 Release
Removed updates related to cnDBTier 24.2.0 as the software is decommissioned and not a valid software for installation or upgrade.

Release 3.24.2 - G11304-06, August 2024

BSF 24.2.0 Release

BSF Known Bugs

Policy 24.2.0 Release

Policy Known Bugs

OCI Adaptor 24.2.0 Release

Compatibility Matrix

Release 3.24.2 - G11304-05, August 2024

BSF 24.2.0 Release

Updated the following sections with the details of BSF release 24.2.0:

- Binding Support Function (BSF)
- Media Pack
- Compatibility Matrix
- 3GPP Compatibility Matrix
- Common Microservices Load Lineup
- BSF Security Certification Declaration
- BSF Resolved Bugs
- BSF Known Bugs

Policy 24.2.0 Release

Updated the following sections with the details of Policy release 24.2.0:

- Policy
- Media Pack
- Compatibility Matrix
- 3GPP Compatibility Matrix
- Common Microservices Load Lineup
- Policy Security Certification Declaration
- Policy Resolved Bugs
- Policy Known Bugs

ATS 24.2.0 Release

Updated the following section with the details of ATS release 24.2.0:

Automated Testing Suite (ATS) Framework

Common Services Resolved Bugs

Updated the following sections with the details of Common Services Resolved Bugs:

- Alternate Route Service Resolved Bugs
- Egress Gateway Resolved Bugs
- Ingress Gateway Resolved Bugs
- Common Configuration Service Resolved Bugs
- Helm Test Resolved Bugs
- NRF-Client Resolved Bugs

Common Services Known Bugs

Updated the following sections with the details of Common Services Known Bugs:

- Egress Gateway Resolved Bugs
- Ingress Gateway Known Bugs

Release 3.24.2 - G11304-04, July 2024

CNE 24.2.0 Release

Updated the following sections with the details of CNE release 24.2.0:

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

OSO 24.2.0 Release

Updated the following sections with the details of OSO release 24.2.0:

- OSO
- Media Pack
- Compatibility Matrix

NEF 24.2.0 Release

Updated the following sections with the details of NEF release 24.2.0:

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

NRF 24.2.0 Release

Updated the following sections with the details of NRF release 24.2.0:

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

NSSF 24.2.0 Release

Updated the following sections with the details of NSSF release 24.2.0:

- Network Slice Selection Function (NSSF)
- Media Pack

- Compatibility Matrix
- 3GPP Compatibility Matrix
- Common Microservices Load Lineup
- NSSF Security Certification Declaration
- NSSF Resolved Bugs
- NSSF Known Bugs

OCI Adaptor 24.2.0 Release

Updated the following sections with the details of OCI Adaptor release 24.2.0:

- OCI Adaptor
- Media Pack

SEPP 24.2.0 Release

Updated the following sections with the details of SEPP release 24.2.0:

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

UDR 24.2.0 Release

Updated the following sections with the details of UDR release 24.2.0:

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

Release 3.24.2 - G11304-02, July 2024

Console 24.2.0 Release

Updated the following sections with the details of Console release 24.2.0:

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

- CNC Console Security Certification Declaration
- CNC Console Resolved Bugs

SCP 24.2.0 Release

Updated the following sections with the details of SCP release 24.2.0:

- Service Communication Proxy (SCP)
- Media Pack
- Compatibility Matrix
- 3GPP Compatibility Matrix
- Common Microservices Load Lineup
- SCP Security Certification Declaration
- SCP Resolved Bugs
- SCP Known Bugs

Release 3.24.2 - G11304-01, July 2024

OCCM 24.2.0 Release

Updated the following sections with the details of OCCM release 24.2.0:

- Oracle Communications Cloud Native Core, Certificate Management (OCCM)
- Media Pack
- Compatibility Matrix
- 3GPP Compatibility Matrix
- Common Microservices Load Lineup
- OCCM Security Certification Declaration
- OCCM Resolved Bugs

1 Introduction

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

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

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

2

Feature Descriptions

This chapter provides a summary of new features and updates to the existing features for network functions released in Cloud Native Core release 3.24.2.

2.1 Automated Testing Suite (ATS) Framework

Release 24.2.0

Oracle Communications Cloud Native Core, Automated Test Suite (ATS) framework 24.2.0 has been updated with the following enhancements:

- **ATS API Enhancement**: With this enhancement, the Starting Jobs API can trigger builds that run all test cases and perform test cases based on specific features, scenarios, stages, groups, and tags. For more information, see "ATS API" in *Oracle Communications Cloud Native Core, Automated Testing Suite Guide.*

2.2 Binding Support Function (BSF)

Release 24.2.3

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

Release 24.2.2

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

Release 24.2.1

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

Release 24.2.0

Oracle Communications Cloud Native Core, Binding Support Function (BSF) 24.2.0 has been updated with the following enhancements:

- **Enhancements to Error Response**: The error responses used to earlier contain only the error description in the details field, which was insufficient to troubleshoot any error. Using the enhanced error response mechanism, BSF sends additional pieces of information such as server FQDN, NF service name, vendor name, and error ID, in the details field of the payload for the identification of the source of an error response. For more information, see "Error response enhancements" section in *Oracle Communications Cloud Native Core, Binding Support Function User Guide*.
- **Support for TLS 1.3**: BSF supports TLS 1.3 for all functions and interfaces that are supported by TLS 1.2. With this feature, BSF supports the creation of TLS 1.3 and TLS 1.2 connections and mandatory ciphers and extensions. For more information, see "Support for TLS 1.3" section in *Oracle Communications Cloud Native Core, Binding Support Function User Guide*.

- **Alert for Stale Session Detection**: New alerts are introduced in BSF 24.2.0 to support auditing of the stale sessions. For more information, see "BSF Alerts" section in *Oracle Communications Cloud Native Core, Binding Support Function User Guide*.
- **Validation Check for nfInstanceID**: For fresh installation of BSF, `nfInstanceId` parameter in the `ocbsf_custom_values_24.2.0.yaml` file should be provided as UUID. During the upgrade, the original UUID or siteID used at the time of installation should be provided. The same global nfInstanceId should be used in the appProfiles as well. For more information,, see "Configuring Mandatory Parameters" section in *Oracle Communications Cloud Native Core, Binding Support Function Installation, Upgrade, and Fault Recovery Guide*.

BSF ATS 24.2.0 is updated with the following enhancement:

- Support for Transport Layer Security: With the introduction of this feature, Jenkins servers have been upgraded to support HTTPS, ensuring a secure and encrypted connection when accessing the ATS dashboard. For more information, see "Deploy ATS with TLS Enabled" section in *Oracle Communications Cloud Native Core, Automated Test Suite Guide*.

2.3 Cloud Native Configuration Console (CNC Console)

Release 24.2.4

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

Release 24.2.3

CNC Console 24.2.3 is a Critical Patch Update. Critical Patch Updates provide security patches for supported Oracle on-premises products. They are available to customers with valid support contracts. For more information, see Critical Patch Updates, Security Alerts and Bulletins.

Release 24.2.2

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

Release 24.2.1

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

Release 24.2.0

Oracle Communications Cloud Native Configuration Console (CNC Console) 24.2.0 includes the following enhancements:

- **Support for TLS v1.3**: Console supports TLS 1.3 for all consumer NFs, producer NFs, the Data Director, SBI Interfaces, and any interfaces that previously supported TLS 1.2. Console uses HTTPS with TLS encryption to establish secure connections with NFs. With this feature, Console supports creation of TLS v1.3 and TLS v1.2 connections and mandatory ciphers and extensions. For more information about this feature, see *Oracle Communications Cloud Native Configuration Console User Guide*.
- **One Manager CNC Console (M-CNCC) to manage NFs located in another M-CNCC Cluster**: In a multicluster deployment, multiple M-CNCCs can exist, and NFs can be located in different M-CNCC clusters. This feature enables one M-CNCC to manage NFs located in another M-CNCC cluster.

- **Support for instance level access control**: This feature enables CNC Console to enforce restrictions on users based on instances allocated to them. If users do not have any instance role assigned, they will not be able to access configuration of that instance. This restriction is in addition to the currently supported RBAC capabilities.
- **CNC Console integration with Common API Framework (CAPIF)**: CNC Console now supports CAPIF, allowing authentication and authorization of API and GUI requests, metrics, alerts, and KPIs. For more information, see the *Oracle Communications Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide* and *Oracle Communications Cloud Native Configuration Console User Guide*.
- **Support for cnDBTier Georeplication Recovery Procedures**: Additional GUI screens have been enabled to perform cnDBTier Georeplication Recovery procedures on CNC Console GUI.
- **NF Versions Supported by CNC Console**:
  - SCP 24.2.x
  - NRF 24.2.x
  - UDR 24.2.x
  - Policy 24.2.x
  - BSF 24.2.x
  - SEPP 24.2.x
  - NSSF 24.2.x
  - NEF 24.2.x
  - CAPIF 24.2.x
  - DD 24.2.x
  - NWDAF 24.2.x
  - OCCM 24.2.x

2.4 Cloud Native Core cnDBTier

Release 24.2.5

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

Release 24.2.4

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

Release 24.2.3

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

Release 24.2.2

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

Release 24.2.1

Oracle Communications Cloud Native Core, cnDBTier (cnDBTier) 24.2.1 includes the following enhancements:

- **cnDBTier Password Encryption**: With this feature, cnDBTier provides an option to encrypt replication username and password stored in the database. This ensures that the passwords stored in the database are secure and are not exposed. When the password encryption feature is enabled, the replication username and password are encrypted throughout the life cycle of cnDBTier unless the feature is disabled. For more information about this feature, see *Oracle Communications Cloud Native Core, cnDBTier User Guide* and *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*.

  > **Note:**
  >
  > cnDBTier supports password encryption from 24.2.1 only. If you have enabled this feature (in the `cutsom_values.yaml` file) in the previous releases, cnDBTier doesn't support upgrade and rollback to 24.2.1. In such a case, disable password encryption in the previous release before performing an upgrade or rollback. For procedure to disable password encryption in the previous release, see the "Disabling Password Encryption" section in *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*.

- **REST APIs to Perform Georeplication Recovery Using CNC Console**: In this release, cnDBTier exposes the following REST APIs to CNC Console:
  - cnDBTier cluster details
  - Get failed cnDBTier clusters
  - Mark cnDBTier clusters as failed
  - Monitor georeplication recovery status
  - Start georeplication recovery

  CNC Console uses these REST APIs to integrate and facilitate users to perform and monitor georeplication recovery using CNC Console. For more information about the REST APIs and procedure to perform georeplication recovery using CNC Console, see *Oracle Communications Cloud Native Core, cnDBTier User Guide* and *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide* respectively.
- **Support for CNE Cloud Native Load Balancer (CNLB)**: With this release, cnDBTier supports network segregation using Cloud Native Load Balancer (CNLB) to effectively manage ingress and egress traffic flows. For more information about this feature, see *Oracle Communications Cloud Native Core, cnDBTier User Guide* and *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*.
- **Enhancement to Georeplication Recovery**: With this enhancement, cnDBTier has improved the rate at which the backup files are transferred between sites during a georeplication recovery. This improvement is achieved by:
  - using Secure File Transfer Protocol (SFTP) instead of CURL to transfer backup files between sites.
  - configuring a separate parameter (`numberofparallelbackuptransfer`) to perform the parallel transfer of backups in the data nodes. For more information about this parameter, see the "Customizing cnDBTier" section in Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide.
- **Support for New Versions of Software**: Oracle MySQL Cluster Database version has been updated to 8.0.37.

2.5 Cloud Native Environment (CNE)

Release 24.2.6

New Versions of Common Services: The version of Ingress nginx is upgraded to 1.11.5.

To get the complete list of third-party services and their versions, refer to the `dependencies_24.2.6.tgz` file provided as part of the software delivery package.

> **Note:**
>
> CNE constitutes a number of third-party services. For information about these third-party services, refer to the documents of the respective third-party services.

Release 24.2.4

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

Release 24.2.3

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

Release 24.2.2

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

Release 24.2.1

Oracle Communications Cloud Native Core, Cloud Native Environment (CNE) 24.2.1 has been updated with the following enhancements:

New Versions of Common Services:

- Rook - 1.15.2

To get the complete list of third-party services and their versions, refer to the `dependencies_24.2.1.tgz` file provided as part of the software delivery package.

Release 24.2.0

Oracle Communications Cloud Native Core, Cloud Native Environment (CNE) 24.2.0 has been updated with the following enhancements:

- **Cloud Native Load Balancer (CNLB)**: With this feature, CNE provides Cloud Native Load Balancer (CNLB), for managing ingress and egress network, as an alternate to the existing LBVM, lb-controller, and egress-controller solution. When this feature is enabled, CNE automatically uses CNLB to control ingress traffic. For managing the egress traffic, you must preconfigure the egress network details in the `cnlb.ini` file before installing CNE. This feature implements a least connection algorithm for IP Virtual Server (IPVS) based ingress distribution.
  For more information about enabling and configuring this feature, see *Oracle Communications Cloud Native Core, Cloud Native Environment User Guide* and *Oracle Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide*.

  Considerations:

  - You can enable or disable this feature only during a fresh installation of CNE 24.2.0.
  - CNE continues to support the existing LBVM, lb-controller, and egress-controller solution for network segregation. If you are using the legacy solution in 24.1.x, you can upgrade to 24.2.0 without any issue. However, if you are freshly installing CNE 24.2.0, you must choose to enable either one of the solutions.

  > **Note:**
  >
  > CNE 24.2.0 replaces Terraform with OpenTofu when you freshly install CNE with Cloud Native Load Balancer (CNLB). For vCNE instances deployed using Terraform, CNE 24.2.0 continues to use and support Terraform for upgrade and maintenance.

- **Support for Network Policies**: With this feature, CNE provides the functionality to define network policies for common services. When network policies are defined on common service pods, the pods can only allow traffic based on the policies defined. This way, the common services are restricted to communicate to trusted sources only. You can enable or disable network policies at the time of installation or upgrade. Network policies are applicable only when CNE runs on LBVM, lb-controller, and egress-controller and not applicable if you are installing CNE with CNLB. For more information about this feature, see *Oracle Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide*.
- **New Versions of Common Services**: The following common services are upgraded in this release:
  - Helm - 3.13.2
  - Kubernetes - 1.29.1
  - containerd - 1.7.13
  - Calico - 3.26.4
  - MetalLB - 0.14.4
  - Prometheus - 2.51.1
  - Grafana - 9.5.3
  - Jaeger - 1.52.0
  - Istio - 1.18.2
  - Kyverno - 1.9
  - cert-manager - 1.12.4

  To get the complete list of third-party services and their versions, refer to the `dependencies_24.2.0.tgz` file provided as part of the software delivery package.

OSO Release 24.2.5

Oracle Communications Operations Services Overlay 24.2.5 has been updated with the following enhancements:

- **Support for Time Series Database (TSDB) Snapshot**: Prometheus uses Time Series Database (TSDB) to store the metrics. Along with metric storage, OSO allows the users to capture a snapshot at a specific point of time with the available data in the Prometheus data store. OSO allows to capture the snapshots without shutting down or disrupting the Prometheus instance. It is useful for taking backups, recovery, or even debugging purposes.

For more information about the feature, see the "Support for Time Series Database (TSDB) Snapshot" section in *Oracle Communications Operations Services Overlay User Guide*.

For more information about capturing the TSDB snapshot procedure, see the "Creating Backups of Prometheus Time Series Database (TSDB) Using Snapshot Utility" section in *Oracle Communications Operations Services Overlay Installation and Upgrade Guide*.

- **Support for new versions**:
  - `24_2_common_pod:latest` is replaced with `24_2_common_oso:24.2.5`
  - `24_2_oso_snapshot:24.2.5`

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

OSO Release 24.2.0

Oracle Communications Operations Services Overlay 24.2.0 has been updated with the following enhancements:

Support for new versions:

- Prometheus is uplifted from version 2.50.1 to 2.52.0.
- alertmanager is uplifted from version 0.26.0 to 0.27.0.
- configmapreload is uplifted from version 0.12.0 to 0.13.0.
- 24_1_common_pod is replaced with 24_2_common_pod.

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

2.6 Oracle Communications Cloud Native Core, Certificate Management (OCCM)

Release 24.2.3

OCCM 24.2.3 is a Critical Patch Update. Critical Patch Updates provide security patches for supported Oracle on-premises products. They are available to customers with valid support contracts. For more information, see Critical Patch Updates, Security Alerts and Bulletins.

Release 24.2.2

OCCM 24.2.2 is a Critical Patch Update. Critical Patch Updates provide security patches for supported Oracle on-premises products. They are available to customers with valid support contracts. For more information, see Critical Patch Updates, Security Alerts and Bulletins.

Release 24.2.1

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

Release 24.2.0

Oracle Communications Cloud Native Core, Certificate Management (OCCM) 24.2.0 includes the following enhancements:

- **Support for Certificate Recreation:** OCCM supports recreation of certificates using existing certificate configuration on the CNC Console GUI. The recreation is supported using the CMPv2 initialization request and response procedures.
  This feature does not support editing the certificate configuration.

2.7 Network Exposure Function (NEF)

Release 24.2.0

Oracle Communications Cloud Native Core, Network Exposure Function (NEF) 24.2.0 includes the following enhancements:

- **Deployment in OCI**: Oracle Cloud Infrastructure (OCI) is a set of complementary cloud services that enable you to build and run a range of applications and services in a High Availability (HA) hosted environment. NEF can be installed or deployed into the OCI using the OCI Adaptor. OCI Adaptor provides a smooth integration of NEF observability and monitoring modules with OCI observability and management, enabling the users to have access of alerts, metrics, and KPIs on the OCI platform.
  For more information on deploying NEF in OCI, see *Oracle Communications Cloud Native Core, Network Exposure Function User Guide, Oracle Communications Cloud Native Core, Network Exposure Function Installation, Upgrade, and Fault Recovery Guide*, *Oracle Communications Cloud Native Core, Network Exposure Function Troubleshooting Guide* and *Oracle Communications Cloud Native Core, OCI Adaptor Deployment Guide*.
- **CAPIF Integration with the CNC Console**: The integration of CAPIF with the CNC Console enables operator to configure and modify different services and features using the CNC Console. For more information, see the "Configuring Network Exposure Function using the CNC Console" section in *Oracle Communications Cloud Native Core, Network Exposure Function User Guide* and *Oracle Communications Cloud Native Core, Network Exposure Function REST Specification Guide*.
- **Support for CNC Top Level MIB in NEF**: There are two MIB files which are used to generate the traps. These files are packaged and shared with the operator in order to fetch the traps in their environment. For more information, see the "Configuring Alert Manager for SNMP Notifier" section in *Oracle Communications Cloud Native Core, Network Exposure Function User Guide*.

2.8 Network Repository Function (NRF)

Release 24.2.4

NRF 24.2.4 is a Critical Patch Update. Critical Patch Updates provide security patches for supported Oracle on-premises products. They are available to customers with valid support contracts.

For more information, see Critical Patch Updates, Security Alerts, and Bulletins.

Oracle Communications Cloud Native Core, Network Repository Functions (NRF) 24.2.4 includes the following enhancements:

- **Egress Gateway Pod Throttling**: With the implementation of this feature, each Egress Gateway pods monitors its incoming traffic and if the traffic exceeds the defined capacity, the excess traffic is not processed and gets rejected. This feature is applied at each pod and applicable to all the incoming requests irrespective of the message type.

> **Note:**
>
> This feature is enabled by default.

For more information about this feature, see the "Egress Gateway Pod Throttling" section in *Oracle Communications Cloud Native Core, Network Repository Function User Guide*.

- **Metrics Enhancements**:
  - **Metric for NfProfile Size**: This metric is introduced to identify the size of the registered NfProfiles.
  - **Metric for NfDiscover response size**: This metric is introduced to determine the size of the NfDiscover response.
    For more information about these metrics, see the "NRF Metrics" section in *Oracle Communications Cloud Native Core, Network Repository Function User Guide*.

Release 24.2.3

NRF 24.2.3 is a Critical Patch Update. Critical Patch Updates provide security patches for supported Oracle on-premises products. They are available to customers with valid support contracts.

For more information, see Critical Patch Updates, Security Alerts, and Bulletins.

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

Release 24.2.2

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

Release 24.2.1

Oracle Communications Cloud Native Core, Network Repository Functions (NRF) 24.2.1 includes the following enhancements:

- **DataSetId Enhancements**: As per 3GPP TS 29.510 v17.7, NRF supports additional enumeration (ENUM) values within DataSetId enumeration. For more information, see the "DataSetId Enhancements" section in *Oracle Communications Cloud Native Core, Network Repository Function User Guide and NRF Compliance Matrix*.
- **Retry Metrics for SLF Flow**: The existing Subscriber Location Function feature is enhanced to track the number of SLF retries made by creating a metric, or updating an existing metric. For more information, see the "SLF Metrics" section in *Oracle Communications Cloud Native Core, Network Repository Function User Guide*.

Release 24.2.0

Oracle Communications Cloud Native Core, Network Repository Functions (NRF) 24.2.0 includes the following enhancements:

- **Support for TLS 1.3**: NRF supports TLS 1.3 for all Consumer NFs, Producer NFs, the Data Director, SBI Interfaces, and any interfaces that previously supported TLS 1.2. NRF uses HTTPS with TLS encryption to establish secure connections with NFs. With this feature, NRF supports creation of TLS v1.3 and TLS v1.2 connections and mandatory ciphers and extensions. For more information about the feature, see the "Support for TLS" section in *Oracle Communications Cloud Native Core, Network Repository Function User Guide* and the "Ingress Gateway Microservice" and "Egress Gateway Microservice" sections in *Oracle Communications Cloud Native Core, Network Repository Function Installation, Upgrade, and Fault Recovery Guide*.

- **Error Log Messages Enhancements**: NRF adds additional information to the existing “`ERROR`” log messages. This additional information can provide more details about the error which can help to identify the problem details, error generating entity, and subscriber information. For more information about the feature, see the "Error Log Messages Enhancements" section in *Oracle Communications Cloud Native Core, Network Repository Function User Guide.*
- **NFService Priority Update**: NRF now updates the NFService level priority along with the NFProfile level priority while processing the discovery query. NRF updates the following:
  - NFProfile level priority considering the lowest NFProfile level priority of NFProfiles
  - NFService level priority considering the lowest NFService level priority of all NFServices

  For more information about this feature, see "NFService Priority Update" section in *Oracle Communications Cloud Native Core, Network Repository Function User Guide*.
- **Rerouting SLF Requests Using Alternate SCP and Alternate SLF**: NRF allows you to configure maximum number of SLF attempts or an alternate SCP route to enhance the routing strategy and minimize the number of reroutes. When an error response is received from SLF, the subsequent reroutes to SLF can be performed using alternate SCP and SLF path. For more information about this feature, see the "Rerouting SLF Requests Using Alternate SCP and Alternate SLF" section in *Oracle Communications Cloud Native Core, Network Repository Function User Guide*.
- **Support for servingScope Attribute in NRF:** As per 3GPP TS 29.510 specification, NRF supports the servingScope for NFProfiles and serving-scope for discovery query attribute. This attribute contains the list of geographical areas that the NF will serve to NRF. This attribute is used to efficiently manage the load distribution among all the producer NfInstances in a network.
  The serving scope is supported for the following service operations:
  - NFRegister
  - NFUpdate (Partial/Complete)
  - NFStatusSubscribe
  - NFDiscover

  For more information about this feature, see *Oracle Communications Cloud Native Core, Network Repository Function Network Impact Report*.

2.9 Network Slice Selection Function (NSSF)

Release 24.2.1

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

Release 24.2.0

Oracle Communications Cloud Native Core, Network Slice Selection Function (NSSF) 24.2.0 includes the following enhancements:

- **Auto-Population of Configuration Based on NSAvailability Update**: This feature has been enhanced in this release by introducing a new set of system options that control its behavior. These options allow administrators to enable or disable the automatic configuration update feature. Additionally, the NSSF can now be configured to receive updates from all AMFs or only from a specified list of trusted AMFs. This flexibility provides granular control over the NSSF's behavior and ensures optimal network slice management. For more information, see "Auto-Population of Configuration Based on NSAvailability Update" section in *Oracle Communications Cloud Native Core, Network Slice Selection Function User Guide*.

- **Enhanced "Update Service Operation" for NSSAI Availability Service of NSSF:** With this enhancement, NSSF now validates NsAvailabilityData from AMFs against its configuration. Only authorized TAI-SNSSAI combinations matching both AMF and NSSF data are accepted, enhancing NSSF's control over processed network availability information. For more information, see "NSSAI Availability Service" section in *Oracle Communications Cloud Native Core, Network Slice Selection Function User Guide*.

2.10 OCI Adaptor

Release 24.2.1

OCI Adaptor 24.2.1 includes the following enhancement:

- **Uplifted the OCI Adapter Components**: The following OCI Adaptor components are upgraded:
  - Management-agent is uplifted from 1.3.0 to 1.5.0.
  - Fluentd is uplifted from 1.4.1 to 1.5.0.
  - Metric-Server is uplifted from 0.6.4 to 0.7.2.
  - OTEL Collector is uplifted from 0.84.0 to 0.108.0.

Release 24.2.0

OCI Adaptor 24.2.0 includes the following enhancements:

- **Supports Configuring Scraping Interval for Application Metrics**: OCI Adaptor allows you to configure scraping interval for application metrics. For more information, see the "Deploying OCI Adaptor" section in *Oracle Communications Cloud Native Core, OCI Adaptor User Guide*.
- **Supports creation of Compartment Admin using the terraforms**: OCI Adaptor supports creation of Compartment Admin group in the OCI infrastructure using terraform script. For more information, see the "User Management Layer" section in *Oracle Communications Cloud Native Core, OCI Deployment Guide*.
- **Replaced Bastion Host VM with Bastion service**: From this release, the Bastion Host VM is replaced with Bastion Service. This allows the users to connect with OKE cluster using CLI server. For more information, see the "Bastion Service" section in *Oracle Communications Cloud Native Core, OCI Deployment Guide*.
- **Supports Configuring App Dimension in metrics data**: OCI Adaptor allows you to include `app` dimension to the metrics of CNC applications. For more information, see the "Deploying OCI Adaptor" section in *Oracle Communications Cloud Native Core, OCI Adaptor User Guide*.
- **Uplifted the OCI Adapter Components**: The following OCI Adaptor components are upgraded:
  - Management-agent is uplifted from 1.0.0 to 1.3.0.
  - Fluentd is uplifted from 1.0.1 to 1.4.1.

2.11 Policy

Release 24.2.6

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

Release 24.2.5

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

Release 24.2.4

Oracle Communications Cloud Native Core, Converged Policy 24.2.4 has been updated with the following enhancements:

- **Traffic Segregation**: Policy supports end-to-end traffic segregation based on traffic types. This ensures that critical networks are not cross-connected or share the same routes, thereby preventing network congestion. For more information, see "*Traffic Segregation*" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.
- **Message Feed for SBI Monitoring**: In order to enable correlation of the internal and external (request/response) messages for all the transactions initiated by the producer and consumer NFs, Policy allows to copy the messages at Ingress and Egress Gateways. The analysis of these messages enable NFs to integrate with external 5G SBI monitoring system for call tracing/tracking and live debugging. For more information about this feature, see "*Message Feed for SBI Monitoring*" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.

Release 24.2.3

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

Release 24.2.2

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

Release 24.2.1

Oracle Communications Cloud Native Core, Converged Policy 24.2.1 has been updated with the following enhancement:

- **Concurrency Handling at Bulwark Service to Reduce Processing Latency of Service Request**: For concurrency handling of different service requests for the same key at the Policy microservice (SM service/PDS), Policy supports reducing the latency of processing different concurrent service requests by acquiring the lock from Bulwark service for failed requests earlier than the backoff timer, rather than waiting for backoff timer to expire. For more information, see "Concurrency Handling at Bulwark Service to Reduce Processing Latency of Service Request" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.
- **Support for Prevention of Requests Accumulation at Undertow Worker Queue**: This functionality helps in preventing accumulation of excessive requests at Undertow worker queue and it is supported by SM, PDS, Binding and Bulwark services. For more information, see "Support for Prevention of Requests Accumulation at Undertow Worker Queue" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.

Release 24.2.0

Oracle Communications Cloud Native Core, Converged Policy 24.2.0 has been updated with the following enhancements:

- **Support for policyDecFailureReports Attribute:** With this feature, PCF supports Policy Decision Error Handling for enabling the *policyDecFailureReports* attribute. For more information, see "Support for policyDecFailureReports Attribute" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.
- **Enhancements to Error Response:** Policy sends error responses to consumer NFs due to some exceptions, such as signaling, validations, and internal errors. These error responses have payloads containing the problem title, status, details, and cause of the error that are used to investigate the error. The details section is now enhanced with application error IDs. For more information about this feature, see "Error response enhancements" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.
- **Enhancements to Concurrency Handling using Bulwark Service in PCRF:** Policy uses the Bulwark service to handle the concurrent requests coming from other Policy services. In this release, Policy has been enhanced to support concurrency handling using bulwark service in PCRF for Rx messages. For more information, see "Support for Concurrency Handling using Bulwark Service in Policy" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.
- **SM Service Pod Congestion Control:** SM service supports Pod Congestion Control mechanism that helps to handle heavy traffic of incoming requests. It considers every incoming request and decides to either reject or accept it based on a defined request priority and the status of service congestion level. For more information, see "SM Service Pod Congestion Control" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.
- **PDS Pod Congestion Control:** PDS service supports Pod Congestion Control mechanism that helps to handle heavy traffic of incoming requests. It considers every incoming request and decides to either reject or accept it based on a defined request priority and the status of service congestion level. For more information, see "PDS Pod Congestion Control" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.
- **Usage Monitoring Pod Congestion Control**: Usage Monitoring service supports Pod Congestion Control mechanism that helps to handle heavy traffic of incoming requests. It considers every incoming request and decides to either reject or accept it based on a defined request priority and the status of service congestion level. For more information, see "Usage Monitoring Service Pod Congestion Control" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.
- **Handling N28 and N36 Interfaces Context Information during Subscription Failures**: With this feature, PCF supports the N28 and N36 context information such as subscription information, policy and charging related information to be stored in PDS database during subscription failures toward CHR or UDR. For more information, see "Handling N28 and N36 Interfaces Context Information during Subscription Failures" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.
- **Support for Optimizing Database Encoding in PCRF Core**: This feature will optimize encoding and decoding of the database fields of PCRF Cores services to reduce the size of data transferred during replication and improve the performance in the call flows. For more information, see "Support for Optimizing Database Encoding in PCRF Core" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.

- **Validation Check for nfInstanceID**: For fresh installation of Policy, `nfInstanceId` parameter in the `occnp_custom_values_occnp_24.2.0.yaml` file should be provided as UUID. During this upgrade, the original UUID or siteID used at time of installation should be provided. The same global `nfInstanceId` should be used in the `appProfiles` as well. For more information, see "Mandatory Configurations" section in *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide*.
- **Support for Handling Reduced Capability Devices**: Policy supports the handling of requests from reduced capability devices (RedCap) to support IoT ecosystem. Policy identifies the incoming request from the RedCap devices and interacts with PRE to make appropriate decisions for the reduced capability devices. For more information, see "Support for Handling Reduced Capability Devices" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.
- **Support for End-to-End Log Identifier across Policy Services**: This feature allows to use a unique identifier to every log message, which can be used to identify the set of logs belonging to a given session across all Policy services. For more information, see "Support for Unique Log Identifier Across Policy Services" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.
- **PCRF Core GxSession Table Multichannel Replication Support**: In order to overcome the replication limitations of the database, especially in a multisite environment, Policy supports slicing the GxSession database. With this database slicing, instead of the main database processing all the requests, some of the database operations are processed using sliced tables. For more information, see "Slicing in GxSession database for PCRF Core service" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.

2.12 Service Communication Proxy (SCP)

Release 24.2.4

SCP 24.2.4 is a Critical Patch Update. Critical Patch Updates provide security patches for supported Oracle on-premises products. They are available to customers with valid support contracts.

For more information, see Critical Patch Updates, Security Alerts, and Bulletins.

Release 24.2.3

SCP 24.2.3 is a Critical Patch Update. Critical Patch Updates provide security patches for supported Oracle on-premises products. They are available to customers with valid support contracts.

For more information, see Critical Patch Updates, Security Alerts, and Bulletins.

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

Release 24.2.2

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

Release 24.2.1

Oracle Communications Cloud Native Core, Service Communication Proxy (SCP) 24.2.1 includes the following enhancement:

Support for 730K MPS: SCP supports traffic at the rate of 730K MPS. For more information, see "Model C - Testcase Scenario 6" in *Oracle Communications Cloud Native Core, Service Communication Proxy Benchmarking Guide*.

Release 24.2.0

Oracle Communications Cloud Native Core, Service Communication Proxy (SCP) 24.2.0 includes the following enhancements:

- **Support for Multiple 3gpp-Sbi-Binding Headers**: With this enhancement, SCP supports multiple 3gpp-Sbi-Binding headers within a single Service-Based Interface (SBI) message, routing them as specified in 3GPP TS 29.500 without additional processing or interpretation. For more information, see "Support for Multiple 3gpp-Sbi-Binding Headers" in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.
- **Support for TLS 1.3**: With this enhancement, SCP strengthens security by extending TLS 1.3 support to all SBI interfaces (consumer NFs, producer NF), the Data Director, and interfaces that previously supported TLS 1.2. SCP uses HTTPS with TLS encryption to establish secure connections with these components. For more information, see "Support for TLS 1.3" in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.
- **Georeplication Recovery API**: With this enhancement, SCP can mark the disrupted cnDBTier cluster as failed, initiate georeplication recovery, and continuously monitor their status, ensuring seamless disaster recovery operations. For more information, see "Support for cnDBTier APIs in CNC Console" in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.
- **Verbose Logging Enhancement**: This enhancement introduces verbose logging specifically for the SCPC-Notification microservice within the control plane. For more information, see "Verbose Logging for SCP" in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.

2.13 Security Edge Protection Proxy (SEPP)

Release 24.2.4

SEPP 24.2.4 is a Critical Patch Update. Critical Patch Updates provide security patches for supported Oracle on-premises products. They are available to customers with valid support contracts.

For more information, see Critical Patch Updates, Security Alerts, and Bulletins.

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

Release 24.2.3

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

Release 24.2.2

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

Release 24.2.1

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

Release 24.2.0

Oracle Communications Cloud Native Core, Security Edge Protection Proxy (SEPP) 24.2.0 includes the following enhancements:

- **Support for Originating Network ID Header Validation, Insertion, and Transposition:** This feature enables the insertion or transposition of either the 3gpp-Sbi-Originating-Network-Id header or the 3gpp-Sbi-Asserted-Plmn-Id header into SBI request messages. It is expected that the originator of a request can be easily identified, but there are some scenarios where the originating network information may not be conveyed in the SBI requests to the home network. In such scenarios, this feature infer the originating PLMN ID and populates the required header in the SBI request.
  The feature supports the following three functionalities:
  - Header Value Validation using Cat 2 Network ID Validation feature
  - Header Addition
  - Header Transposition

  For more information about the feature, see *Oracle Communications Cloud Native Core, Security Edge Protection Proxy User Guid*e, *Oracle Communications Cloud Native Core, Security Edge Protection Proxy REST API Guide*, and Oracle Communications Cloud Native Core, Security Edge Protection Proxy Troubleshooting Guide.
- **Supports Four-Site Georedundancy:** Oracle Communications Cloud Native Core, Security Edge Protection Proxy (SEPP) now supports four-site georedundancy. SEPP offers a two, three, or four-sites georedundancy to ensure service availability when one of the SEPP sites is down. When SEPP is deployed as georedundant site, all the sites work in an active state and the same data is available at all the sites.
  For more information about the feature, see the "Georedundancy" section in *Oracle Communications Cloud Native Core, Security Edge Protection Proxy User Guide*.
- **Support for Georeplication Recovery cnDBTier APIs in CNC Console**: With this enhancement, Georeplication Recovery cnDBTier APIs are integrated into the CNC Console, and users can view specific cnDBTier statuses on the CNC Console.
  For more information about the feature, see the "Support for cnDBTier APIs in CNC Console" and "cnDBTier" sections in *Oracle Communications Cloud Native Core, Security Edge Protection Proxy User Guide.*
- **Support for Common Service APIs in CNC Console**: The configuration for Ingress Gateway and Egress Gateway APIs was earlier supported only using REST. With the implementation of this feature, SEPP now supports the configuration of Ingress Gateway and Egress Gateway APIs using the CNC Console.
  For more information about the feature, see the "Support for Common Service APIs in CNC Console" and "Configurations" sections in *Oracle Communications Cloud Native Core, Security Edge Protection Proxy User Guide.*
- **ATS APIs**: The Application Programming Interface (API) feature provides APIs to perform routine ATS tasks as follows:
  - Start: To initiate one of the three test suites, such as Regression, New Features, or Performance.
  - Monitor: To obtain the progress of a test suite's execution.
  - Stop: To cancel an active test suite.
  - Get Artifacts: To retrieve the JUNIT format XML test result files for a completed test suite.

For more information about the feature, see 'ATS Framework Features' section in *Oracle Communications Cloud Native Core, Automated Testing Suite Guide.*

2.14 Unified Data Repository (UDR)

Release 24.2.5

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

Release 24.2.4

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

Release 24.2.3

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

Release 24.2.2

Oracle Communications Cloud Native Core, Unified Data Repository (UDR) 24.2.2 includes the following enhancements:

- **Support for Post Operation for an Existing Subscription**: This feature enables UDR to support POST request that overwrites the existing subscription. For more information, see "Support for Post Operation for an Existing Subscription" section in *Oracle Communications Cloud Native Core, Unified Data Repository User Guide*.

Release 24.2.1

Oracle Communications Cloud Native Core, Unified Data Repository (UDR) 24.2.1 includes the following enhancements:

- **Secure File Transfer Support for Subscriber Bulk Import Tool Enhancement**: This feature is enhanced to support separate file paths for PDBI files and result log files. For more information, see "Secure File Transfer Support for Subscriber Bulk Import Tool Enhancement" section in *Oracle Communications Cloud Native Core, Unified Data Repository User Guide*.

Release 24.2.0

Oracle Communications Cloud Native Core, Unified Data Repository (UDR) 24.2.0 includes the following enhancements:

- **Support for Automated PKI Integration**: UDR supports automation of certificate lifecycle management in integration with Oracle Communications Certificate Manager (OCCM). This allows to automatically create, renew, and delete certificates for a given CA, with the possibility to track previously created certificates and renew/delete them when required. For more information about the feature, see "Support for Automated PKI Integration" section in *Oracle Communications Cloud Native Core, Unified Data Repository User Guide.*
- **Suppress Notification**: This feature enables cnUDR to store the User-Agent header received in the POST request from cnPCRF in the subscription table. cnUDR compares the User-Agent header received during an update operation from cnPCRF with the stored User-Agent header. If the User-Agent header match, then the notification is suppressed. The notification is sent if the User-Agent headers do not match or if the there is no User-Agent header in the update request. For more information about the feature, see "Suppress Notification" section in *Oracle Communications Cloud Native Core, Unified Data Repository User Guide.*

- **Support for Common Service APIs in CNC Console**: The configuration for common service APIs was earlier supported only using REST API. With the implementation of this feature, UDR now supports the configuration of Ingress Gateway and Egress Gateway parameters using the CNC Console. For more information about the feature, see "Support for Common Service APIs in CNC Console" section in *Oracle Communications Cloud Native Core, Unified Data Repository User Guide.*
- **Support for TLS v1.3**: UDR supports TLS 1.3 for all Consumer NFs, Producer NFs, the Data Director, SBI Interfaces, and any interfaces that previously supported TLS 1.2. UDR uses HTTPS with TLS encryption to establish secure connections with NFs. With this feature, UDR supports creation of TLS v1.3 and TLS v1.2 connections and mandatory ciphers and extensions. For more information about the feature, see "Support for TLS" section in *Oracle Communications Cloud Native Core, Unified Data Repository User Guide.*
- **Error Logging Enhancement**: With this feature, UDR sends additional information to the existing “ERROR” log messages to identify the cause of the issue and minimize the troubleshooting time. Additional attributes are added to the existing ERROR logs which get populated with appropriate values during failure scenarios. For more information about the feature, see "Error Logging Enhancement" section in *Oracle Communications Cloud Native Core, Unified Data Repository User Guide.*

3
Media and Documentation

3.1 Media Pack

This section lists the media package for Oracle Communications Cloud Native Core 3.24.2. To download the media package, see MOS.

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

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

Table 3-1 Media Pack Contents for Oracle Communications Cloud Native Core 3.24.2

Description	NF Version	ATS Version	Upgrade Supported
Oracle Communications Cloud Native Core, Binding Support Function (BSF)	24.2.3	24.2.3	BSF 24.2.3 supports fresh installation and upgrade from 24.2.x, 24.1.x, and 23.4.x. For more information, see *Oracle Communications Cloud Native Core, Binding Support Function Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Binding Support Function (BSF)	24.2.2	24.2.2	BSF 24.2.2 supports fresh installation and upgrade from 24.2.x, 24.1.x, and 23.4.x. For more information, see *Oracle Communications Cloud Native Core, Binding Support Function Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Binding Support Function (BSF)	24.2.1	24.2.1	BSF 24.2.1 supports fresh installation and upgrade from 24.2.0, 24.1.x, and 23.4.x. For more information, see *Oracle Communications Cloud Native Core, Binding Support Function Installation, Upgrade, and Fault Recovery Guide*.

Table 3-1 (Cont.) Media Pack Contents for Oracle Communications Cloud Native Core 3.24.2

Description	NF Version	ATS Version	Upgrade Supported
Oracle Communications Cloud Native Core, Binding Support Function (BSF)	24.2.0	24.2.0	BSF 24.2.0 supports fresh installation and upgrade from 24.1.x and 23.4.x. For more information, see *Oracle Communications Cloud Native Core, Binding Support Function Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Configuration Console (CNC Console)	24.2.4	NA	CNC Console 24.2.4 supports fresh installation and upgrade from 24.2.x, 24.1.x, and 23.4.x. For more information, see *Oracle Communications Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide.* **Note**: CNC Console supports N-2 NF versions during the upgrade window. For example, CNC Console 24.2.x supports SCP 24.2.x, 24.1.x, and 23.4.x. Any newly added features in Console that have NF dependency in the latest release may not be available in the previous release.
Oracle Communications Cloud Native Configuration Console (CNC Console)	24.2.3	NA	CNC Console 24.2.3 supports fresh installation and upgrade from 24.2.x, 24.1.x, and 23.4.x. For more information, see *Oracle Communications Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide.* **Note**: CNC Console supports N-2 NF versions during the upgrade window. For example, CNC Console 24.2.x supports SCP 24.2.x, 24.1.x, and 23.4.x. Any newly added features in Console that have NF dependency in the latest release may not be available in the previous release.

Table 3-1 (Cont.) Media Pack Contents for Oracle Communications Cloud Native Core 3.24.2

Description	NF Version	ATS Version	Upgrade Supported
Oracle Communications Cloud Native Configuration Console (CNC Console)	24.2.2	NA	CNC Console 24.2.2 supports fresh installation and upgrade from 24.2.x, 24.1.x, and 23.4.x. For more information, see *Oracle Communications Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide.* **Note**: CNC Console supports N-2 NF versions during the upgrade window. For example, CNC Console 24.2.x supports SCP 24.2.x, 24.1.x, and 23.4.x. Any newly added features in Console that have NF dependency in the latest release may not be available in the previous release.
Oracle Communications Cloud Native Configuration Console (CNC Console)	24.2.1	NA	CNC Console 24.2.1 supports fresh installation and upgrade from 24.2.0, 23.4.x, and 24.1.x. For more information, see *Oracle Communications Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Configuration Console (CNC Console)	24.2.0	NA	CNC Console 24.2.0 supports fresh installation and upgrade from 23.4.x and 24.1.x. For more information, see *Oracle Communications Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide.*
Oracle Communications Cloud Native Core, cnDBTier (cnDBTier)	24.2.5	NA	cnDBTier 24.2.5 supports fresh installation and upgrade from 24.2.x, 24.1.x, and 23.4.x. For more information, see Oracle Communications Cloud Native Core, *cnDBTier Installation, Upgrade, and Fault Recovery Guide.* **Note**: • cnDBTier supports upgrade to 24.2.5 only if password encryption is disabled in the version that is being upgraded. • cnDBTier supports rollback to 24.1.x and 23.4.x only if password encryption is disabled in the version that is being rolled back.

Table 3-1 (Cont.) Media Pack Contents for Oracle Communications Cloud Native Core 3.24.2

Description	NF Version	ATS Version	Upgrade Supported
Oracle Communications Cloud Native Core, cnDBTier (cnDBTier)	24.2.4	NA	cnDBTier 24.2.4 supports fresh installation and upgrade from 24.2.x, 24.1.x, and 23.4.x. For more information, see Oracle Communications Cloud Native Core, *cnDBTier Installation, Upgrade, and Fault Recovery Guide.* **Note**: • cnDBTier supports upgrade to 24.2.4 only if password encryption is disabled in the version that is being upgraded. • cnDBTier supports rollback to 24.1.x and 23.4.x only if password encryption is disabled in the version that is being rolled back.
Oracle Communications Cloud Native Core, cnDBTier (cnDBTier)	24.2.3	NA	cnDBTier 24.2.3 supports fresh installation and upgrade from 24.2.x, 24.1.x, and 23.4.x. For more information, see *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*. **Note**: • cnDBTier supports upgrade to 24.2.3 only if password encryption is disabled in the version that is being upgraded. • cnDBTier supports rollback to 24.1.x and 23.4.x only if password encryption is disabled in the version that is being rolled back.

Table 3-1 (Cont.) Media Pack Contents for Oracle Communications Cloud Native Core 3.24.2

Description	NF Version	ATS Version	Upgrade Supported
Oracle Communications Cloud Native Core, cnDBTier (cnDBTier)	24.2.2	NA	cnDBTier 24.2.2 supports fresh installation and upgrade from 23.4.x, 24.1.x, and 24.2.x. For more information, see *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*. **Note:** cnDBTier doesn't support upgrade and rollback if password encryption is enabled (in the `cutsom_values.yaml` file) in the previous release. In such a case, disable password encryption in the previous release before performing an upgrade or rollback. For procedure to disable password encryption in the previous release, see the "Disabling Password Encryption" section in *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, cnDBTier (cnDBTier)	24.2.1	NA	cnDBTier 24.2.1 supports fresh installation and upgrade from 23.4.x and 24.1.x. For more information, see *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*. **Note:** cnDBTier doesn't support upgrade and rollback if password encryption is enabled (in the `cutsom_values.yaml` file) in the previous release. In such a case, disable password encryption in the previous release before performing an upgrade or rollback. For procedure to disable password encryption in the previous release, see the "Disabling Password Encryption" section in *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*.

Table 3-1 (Cont.) Media Pack Contents for Oracle Communications Cloud Native Core 3.24.2

Description	NF Version	ATS Version	Upgrade Supported
Oracle Communications Cloud Native Core, cnDBTier (cnDBTier)	24.2.0	NA	cnDBTier 24.2.0 supports fresh installation and upgrade from 23.4.x and 24.1.x. For more information, see *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*. **Note:** cnDBTier doesn't support upgrade and rollback if password encryption is enabled (in the `cutsom_values.yaml` file) in the previous release. In such a case, disable password encryption in the previous release before performing an upgrade or rollback. For procedure to disable password encryption in the previous release, see the "Disabling Password Encryption" section in *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Cloud Native Environment (CNE)	24.2.6	NA	CNE 24.2.6 supports fresh installation and upgrade from 24.1.x and 24.2.x. For more information, see *Oracle Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Cloud Native Environment (CNE)	24.2.4	NA	CNE 24.2.4 supports fresh installation and upgrade from 24.1.x and 24.2.x. For more information, see *Oracle Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Cloud Native Environment (CNE)	24.2.3	NA	CNE 24.2.3 supports fresh installation and upgrade from 24.1.x and 24.2.x. For more information, see *Oracle Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Cloud Native Environment (CNE)	24.2.2	NA	CNE 24.2.2 supports fresh installation and upgrade from 24.1.x and 24.2.x. For more information, see *Oracle Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide*.

Table 3-1 (Cont.) Media Pack Contents for Oracle Communications Cloud Native Core 3.24.2

Description	NF Version	ATS Version	Upgrade Supported
Oracle Communications Cloud Native Core, Cloud Native Environment (CNE)	24.2.1	NA	CNE 24.2.1 supports fresh installation and upgrade from 24.1.x and 24.2.x. For more information, see *Oracle Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Cloud Native Environment (CNE)	24.2.0	NA	CNE 24.2.0 supports fresh installation and upgrade from 24.1.x. For more information, see *Oracle Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Network Exposure Function (NEF)	24.2.0	24.2.0	NEF 24.2.0 supports fresh installation and upgrade from 24.1.x and 23.4.x. For more information, see *Oracle Communications Cloud Native Core, Network Exposure Function Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Network Repository Function (NRF)	24.2.4	24.2.4	NRF 24.2.4 supports fresh installation and upgrade from 24.1.x and 24.2.x. For more information, see *Oracle Communications Cloud Native Core, Network Repository Function Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Network Repository Function (NRF)	24.2.3	24.2.3	NRF 24.2.3 supports fresh installation and upgrade from 24.1.x and 24.2.x. For more information, see *Oracle Communications Cloud Native Core, Network Repository Function Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Network Repository Function (NRF)	24.2.2	24.2.2	NRF 24.2.2 supports fresh installation and upgrade from 24.1.x and 24.2.x. For more information, see *Oracle Communications Cloud Native Core, Network Repository Function Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Network Repository Function (NRF)	24.2.1	24.2.1	NRF 24.2.1 supports fresh installation and upgrade from 24.1.x and 24.2.x. For more information, see *Oracle Communications Cloud Native Core, Network Repository Function Installation, Upgrade, and Fault Recovery Guide*.

Table 3-1 (Cont.) Media Pack Contents for Oracle Communications Cloud Native Core 3.24.2

Description	NF Version	ATS Version	Upgrade Supported
Oracle Communications Cloud Native Core, Network Repository Function (NRF)	24.2.0	24.2.0	NRF 24.2.0 supports fresh installation and upgrade from 24.1.x. For more information, see *Oracle Communications Cloud Native Core, Network Repository Function Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Network Slice Selection Function (NSSF)	24.2.1	24.2.0	NSSF 24.2.1 supports fresh installation and upgrade from 24.2.0 and 24.1.x. For more information, see *Oracle Communications Cloud Native Core, Network Slice Selection Function Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Network Slice Selection Function (NSSF)	24.2.0	24.2.0	NSSF 24.2.0 supports fresh installation and upgrade from 24.1.x. For more information, see *Oracle Communications Cloud Native Core, Network Slice Selection Function Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Certificate Management (OCCM)	24.2.3	NA	OCCM 24.2.3 supports fresh installation and upgrade from 24.2.x, 24.1.x, and 23.4.x. For more information, see *Oracle Communications Cloud Native Core, Certificate Management Installation, Upgrade, and Fault Recovery Guide.*
Oracle Communications Cloud Native Core, Certificate Management (OCCM)	24.2.2	NA	OCCM 24.2.2 supports fresh installation and upgrade from 24.2.x, 24.1.x, and 23.4.x. For more information, see *Oracle Communications Cloud Native Core, Certificate Management Installation, Upgrade, and Fault Recovery Guide.*
Oracle Communications Cloud Native Core, Certificate Management (OCCM)	24.2.1	NA	OCCM 24.2.1 supports fresh installation and upgrade from 24.2.0, 24.1.x, and 23.4.x. For more information, see *Oracle Communications Cloud Native Core, Certificate Management Installation, Upgrade, and Fault Recovery Guide.*
Oracle Communications Cloud Native Core, Certificate Management (OCCM)	24.2.0	NA	OCCM 24.2.0 supports fresh installation and upgrade from 23.4.x and 24.1.x. For more information, see *Oracle Communications Cloud Native Core, Certificate Management Installation, Upgrade, and Fault Recovery Guide.*

Table 3-1 (Cont.) Media Pack Contents for Oracle Communications Cloud Native Core 3.24.2

Description	NF Version	ATS Version	Upgrade Supported
Oracle Communications Cloud Native Core, OCI Adaptor	24.2.1	NA	OCI Adaptor supports fresh installation only.
Oracle Communications Cloud Native Core, OCI Adaptor	24.2.0	NA	OCI Adaptor supports fresh installation only.
Oracle Communications Operations Services Overlay (OSO)	24.2.5	NA	OSO 24.2.5 supports fresh installation and upgrade from 24.2.x and 24.1.x. For more information, see *Oracle Communications Operations Services Overlay Installation and Upgrade Guide*.
Oracle Communications Operations Services Overlay (OSO)	24.2.0	NA	OSO 24.2.0 supports fresh installation and upgrade from 24.1.x. For more information, see *Oracle Communications Operations Services Overlay Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core, Converged Policy (Policy)	24.2.6	24.2.5	Policy 24.2.6 supports fresh installation and upgrade from 24.2.x, 24.1.x, and 23.4.x. For more information, see *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Converged Policy (Policy)	24.2.5	24.2.5	Policy 24.2.5 supports fresh installation and upgrade from 24.2.x, 24.1.x, and 23.4.x. For more information, see *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Converged Policy (Policy)	24.2.4	24.2.4	Policy 24.2.4 supports fresh installation and upgrade from 24.2.x, 24.1.x, and 23.4.x. For more information, see *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Converged Policy (Policy)	24.2.3	24.2.3	Policy 24.2.3 supports fresh installation and upgrade from 24.2.x, 24.1.x, and 23.4.x. For more information, see *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide*.

Table 3-1 (Cont.) Media Pack Contents for Oracle Communications Cloud Native Core 3.24.2

Description	NF Version	ATS Version	Upgrade Supported
Oracle Communications Cloud Native Core, Converged Policy (Policy)	24.2.2	24.2.2	Policy 24.2.2 supports fresh installation and upgrade from 24.2.x, 24.1.x, and 23.4.x. For more information, see *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Converged Policy (Policy)	24.2.1	24.2.1	Policy 24.2.1 supports fresh installation and upgrade from 24.2.0, 24.1.x, and 23.4.x. For more information, see *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Converged Policy (Policy)	24.2.0	24.2.0	Policy 24.2.0 supports fresh installation and upgrade from 24.1.x and 23.4.x. For more information, see *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Service Communications Proxy (SCP)	24.2.4	24.2.4	SCP 24.2.4 supports fresh installation and upgrade from 23.4.x, 24.1.x, and 24.2.x. For more information, see *Oracle Communications Cloud Native Core, Service Communication Proxy Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Service Communications Proxy (SCP)	24.2.3	24.2.3	SCP 24.2.3 supports fresh installation and upgrade from 23.4.x, 24.1.x, and 24.2.x. For more information, see *Oracle Communications Cloud Native Core, Service Communication Proxy Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Service Communications Proxy (SCP)	24.2.2	24.2.2	SCP 24.2.2 supports fresh installation and upgrade from 23.4.x, 24.1.x, and 24.2.x. For more information, see *Oracle Communications Cloud Native Core, Service Communication Proxy Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Service Communications Proxy (SCP)	24.2.1	24.2.1	SCP 24.2.1 supports fresh installation and upgrade from 23.4.x, 24.1.x, and 24.2.x. For more information, see *Oracle Communications Cloud Native Core, Service Communication Proxy Installation, Upgrade, and Fault Recovery Guide*.

Table 3-1 (Cont.) Media Pack Contents for Oracle Communications Cloud Native Core 3.24.2

Description	NF Version	ATS Version	Upgrade Supported
Oracle Communications Cloud Native Core, Service Communications Proxy (SCP)	24.2.0	24.2.0	SCP 24.2.0 supports fresh installation and upgrade from 23.4.x and 24.1.x. For more information, see *Oracle Communications Cloud Native Core, Service Communication Proxy Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Security Edge Protection Proxy (SEPP)	24.2.4	24.2.4	SEPP 24.2.4 supports fresh installation and upgrade from 24.2.x, 24.1.x, and 23.4.x. For more information, see *Oracle Communications Cloud Native Core, Security Edge Protection Proxy Installation, Upgrade, and Fault Recovery Guide.*
Oracle Communications Cloud Native Core, Security Edge Protection Proxy (SEPP)	24.2.3	24.2.3	SEPP 24.2.3 supports fresh installation and upgrade from 24.2.x, 24.1.x, and 23.4.x. For more information, see *Oracle Communications Cloud Native Core, Security Edge Protection Proxy Installation, Upgrade, and Fault Recovery Guide.*
Oracle Communications Cloud Native Core, Security Edge Protection Proxy (SEPP)	24.2.2	24.2.2	SEPP 24.2.2 supports fresh installation and upgrade from 24.2.x, 24.1.x, and 23.4.x. For more information, see *Oracle Communications Cloud Native Core, Security Edge Protection Proxy Installation, Upgrade, and Fault Recovery Guide.*
Oracle Communications Cloud Native Core, Security Edge Protection Proxy (SEPP)	24.2.1	24.2.1	SEPP 24.2.1 supports fresh installation and upgrade from 24.2.0, 24.1.x, and 23.4.x. For more information, see *Oracle Communications Cloud Native Core, Security Edge Protection Proxy Installation, Upgrade, and Fault Recovery Guide.*
Oracle Communications Cloud Native Core, Security Edge Protection Proxy (SEPP)	24.2.0	24.2.0	SEPP 24.2.0 supports fresh installation and upgrade from 24.1.x, and 23.4.x. For more information, see *Oracle Communications Cloud Native Core, Security Edge Protection Proxy Installation, Upgrade, and Fault Recovery Guide.*

Table 3-1 (Cont.) Media Pack Contents for Oracle Communications Cloud Native Core 3.24.2

Description	NF Version	ATS Version	Upgrade Supported
Oracle Communications Cloud Native Core, Unified Data Repository (UDR)	24.2.5	24.2.5	UDR 24.2.5 supports fresh installation and upgrade from 24.2.x, 24.1.x, and 23.4.x. For more information, see *Oracle Communications Cloud Native Core, Unified Data Repository Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Unified Data Repository (UDR)	24.2.4	24.2.4	UDR 24.2.4 supports fresh installation and upgrade from 24.2.x, 24.1.x, and 23.4.x. For more information, see *Oracle Communications Cloud Native Core, Unified Data Repository Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Unified Data Repository (UDR)	24.2.3	24.2.3	UDR 24.2.3 supports fresh installation and upgrade from 24.2.x, 24.1.x, and 23.4.x. For more information, see *Oracle Communications Cloud Native Core, Unified Data Repository Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Unified Data Repository (UDR)	24.2.2	24.2.2	UDR 24.2.2 supports fresh installation and upgrade from 24.2.x, 24.1.x, and 23.4.x. For more information, see Oracle Communications Cloud Native Core, Unified Data Repository Installation, Upgrade, and Fault Recovery Guide.
Oracle Communications Cloud Native Core, Unified Data Repository (UDR)	24.2.1	24.2.1	UDR 24.2.1 supports fresh installation and upgrade from 24.2.0, 24.1.x, and 23.4.x. For more information, see Oracle Communications Cloud Native Core, Unified Data Repository Installation, Upgrade, and Fault Recovery Guide.
Oracle Communications Cloud Native Core, Unified Data Repository (UDR)	24.2.0	24.2.0	UDR 24.2.0 supports fresh installation and upgrade from 23.4.x, and 24.1.x. For more information, see Oracle Communications Cloud Native Core, Unified Data Repository Installation, Upgrade, and Fault Recovery Guide.

3.2 Compatibility Matrix

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

Note:

- Removed the NFs' compatibility details with CDCS from the "Compatibility Matrix" table as the CNC no longer supports Oracle Communications CD Control Server (CDCS).
- For seamless integration and optimal performance of CNC NFs on third party platform, the third party platform needs to be compatible with the specified Kubernetes version.

Table 3-2 Compatibility Matrix

CNC NF	NF Version	CNE	cnDBTier	OSO	ASM S/W	Kubernetes	CNC Console	OCNADD	OCCM	OCI Adaptor
BSF	24.2.3	• 24.2.x • 24.1.x • 23.4.x	• 24.2.x • 24.1.x • 23.4.x	• 24.2.x • 24.1.x • 23.4.x	1.14.6	• 1.29.x • 1.28.x • 1.27.x	24.2.x	NA	24.2.x	NA
BSF	24.2.2	• 24.2.x • 24.1.x • 23.4.x	• 24.2.x • 24.1.x • 23.4.x	• 24.2.x • 24.1.x • 23.4.x	1.14.6	• 1.29.x • 1.28.x • 1.27.x	24.2.x	NA	24.2.x	NA
BSF	24.2.1	• 24.2.x • 24.1.x • 23.4.x	• 24.2.x • 24.1.x • 23.4.x	• 24.2.x • 24.1.x • 23.4.x	1.14.6	• 1.29.x • 1.28.x • 1.27.x	24.2.x	NA	24.2.x	NA
BSF	24.2.0	• 24.2.x • 24.1.x • 23.4.x	• 24.2.x • 24.1.x • 23.4.x	• 24.2.x • 24.1.x • 23.4.x	1.14.6	• 1.29.x • 1.28.x • 1.27.x	24.2.x	NA	24.2.x	NA

Table 3-2 (Cont.) Compatibility Matrix

CNC NF	NF Version	CNE	cnDBTier	OSO	ASM S/W	Kubernetes	CNC Console	OCNADD	OCCM	OCI Adaptor
CNC Console	24.2.4	• 24.2.x • 24.1.x • 23.4.x	• 24.2.x • 24.1.x • 23.4.x	• 24.2.x • 24.1.x • 23.4.x	• 1.14.6 • 1.11.8 • 1.9.8	• 1.29.x • 1.28.x • 1.27.x	NA	24.2.x	24.2.x	24.2.x
CNC Console	24.2.3	• 24.2.x • 24.1.x • 23.4.x	• 24.2.x • 24.1.x • 23.4.x	• 24.2.x • 24.1.x • 23.4.x	• 1.14.6 • 1.11.8 • 1.9.8	• 1.29.x • 1.28.x • 1.27.x	NA	24.2.x	24.2.x	24.2.x
CNC Console	24.2.2	• 24.2.x • 24.1.x • 23.4.x	• 24.2.x • 24.1.x • 23.4.x	• 24.2.x • 24.1.x • 23.4.x	• 1.14.6 • 1.11.8 • 1.9.8	• 1.29.x • 1.28.x • 1.27.x	NA	24.2.x	24.2.x	24.2.x
CNC Console	24.2.1	• 24.2.x • 24.1.x • 23.4.x	• 24.2.x • 24.1.x • 23.4.x	• 24.2.x • 24.1.x • 23.4.x	• 1.14.6 • 1.11.8 • 1.9.8	• 1.29.x • 1.28.x • 1.27.x	NA	24.2.x	24.2.x	24.2.x
CNC Console	24.2.0	• 24.2.x • 24.1.x • 23.4.x	• 24.2.x • 24.1.x • 23.4.x	• 24.2.x • 24.1.x • 23.4.x	• 1.14.6 • 1.11.8 • 1.9.8	• 1.29.x • 1.28.x • 1.27.x	NA	24.2.x	24.2.x	24.2.x
cnDBTier	24.2.5	• 24.2.x • 24.1.x • 23.4.x	NA	NA	NA	• 1.29.x • 1.28.x • 1.27.x	NA	NA	NA	NA

Table 3-2 (Cont.) Compatibility Matrix

CNC NF	NF Version	CNE	cnDBTier	OSO	ASM S/W	Kubernetes	CNC Console	OCNADD	OCCM	OCI Adaptor
cnDBTier	24.2.4	• 24.2.x • 24.1.x • 23.4.x	NA	NA	NA	• 1.29.x • 1.28.x • 1.27.x	NA	NA	NA	NA
cnDBTier	24.2.3	• 24.2.x • 24.1.x • 23.4.x	NA	NA	NA	• 1.29.x • 1.28.x • 1.27.x	NA	NA	NA	NA
cnDBTier	24.2.2	• 24.2.x • 24.1.x • 23.4.x	NA	NA	NA	• 1.29.x • 1.28.x • 1.27.x	NA	NA	NA	NA
cnDBTier	24.2.1	• 24.2.x • 24.1.x • 23.4.x	NA	NA	NA	• 1.29.x • 1.28.x • 1.27.x	NA	NA	NA	NA
cnDBTier	24.2.0	• 24.2.x • 24.1.x • 23.4.x	NA	NA	NA	• 1.29.x • 1.28.x • 1.27.x	NA	NA	NA	NA
CNE	24.2.6	NA	NA	NA	NA	1.29.x	NA	NA	NA	NA
CNE	24.2.4	NA	NA	NA	NA	1.29.x	NA	NA	NA	NA
CNE	24.2.3	NA	NA	NA	NA	1.29.x	NA	NA	NA	NA
CNE	24.2.2	NA	NA	NA	NA	1.29.x	NA	NA	NA	NA
CNE	24.2.1	NA	NA	NA	NA	1.29.x	NA	NA	NA	NA
CNE	24.2.0	NA	NA	NA	NA	1.29.x	NA	NA	NA	NA
NEF	24.2.0	• 24.2.x • 24.1.x • 23.4.x	• 24.2.x • 24.1.x • 23.4.x	NA	NA	• 1.29.x • 1.28.x • 1.27.x	24.2.x	NA	NA	24.2.x

Table 3-2 (Cont.) Compatibility Matrix

CNC NF	NF Version	CNE	cnDBTier	OSO	ASM S/W	Kubernetes	CNC Console	OCNADD	OCCM	OCI Adaptor
NRF	24.2.4	• 24.2.x • 24.1.x • 23.4.x	• 24.2.x • 24.1.x • 23.4.x	• 24.2.x • 24.1.x • 23.4.x	1.14.6	• 1.29.x • 1.28.x • 1.27.x	24.2.x	24.2.x	24.2.x	24.2.x
NRF	24.2.3	• 24.2.x • 24.1.x • 23.4.x	• 24.2.x • 24.1.x • 23.4.x	• 24.2.x • 24.1.x • 23.4.x	1.14.6	• 1.29.x • 1.28.x • 1.27.x	24.2.x	24.2.x	24.2.x	24.2.x
NRF	24.2.2	• 24.2.x • 24.1.x • 23.4.x	• 24.2.x • 24.1.x • 23.4.x	• 24.2.x • 24.1.x • 23.4.x	1.14.6	• 1.29.x • 1.28.x • 1.27.x	24.2.x	24.2.x	24.2.x	24.2.x
NRF	24.2.1	• 24.2.x • 24.1.x • 23.4.x	• 24.2.x • 24.1.x • 23.4.x	• 24.2.x • 24.1.x • 23.4.x	1.14.6	• 1.29.x • 1.28.x • 1.27.x	24.2.x	24.2.x	24.2.x	24.2.x
NRF	24.2.0	• 24.2.x • 24.1.x • 23.4.x	• 24.2.x • 24.1.x • 23.4.x	• 24.2.x • 24.1.x • 23.4.x	1.14.6	• 1.29.x • 1.28.x • 1.27.x	24.2.x	24.2.x	24.2.x	24.2.x

Table 3-2 (Cont.) Compatibility Matrix

CNC NF	NF Version	CNE	cnDBTier	OSO	ASM S/W	Kubernetes	CNC Console	OCNADD	OCCM	OCI Adaptor
NSSF	24.2.1	- 24.2.x - 24.1.x - 23.4.x	- 24.2.x - 24.1.x - 23.4.x	- 24.2.x - 24.1.x - 23.4.x	- 1.14.6 - 1.11.8	- 1.29.x - 1.28.x - 1.27.x	24.2.x	NA	NA	NA
NSSF	24.2.0	- 24.2.x - 24.1.x - 23.4.x	- 24.2.x - 24.1.x - 23.4.x	- 24.2.x - 24.1.x - 23.4.x	- 1.14.6 - 1.11.8	- 1.29.x - 1.28.x - 1.27.x	24.2.x	NA	NA	NA
OCCM	24.2.3	- 24.2.x - 24.1.x - 23.4.x	NA	NA	NA	- 1.29.x - 1.28.x - 1.27.x	24.2.x	NA	NA	NA
OCCM	24.2.2	- 24.2.x - 24.1.x - 23.4.x	NA	NA	NA	- 1.29.x - 1.28.x - 1.27.x	24.2.x	NA	NA	NA
OCCM	24.2.1	- 24.2.x - 24.1.x - 23.4.x	NA	NA	NA	- 1.29.x - 1.28.x - 1.27.x	24.2.x	NA	NA	NA
OCCM	24.2.0	- 24.2.x - 24.1.x - 23.4.x	NA	NA	NA	- 1.29.x - 1.28.x - 1.27.x	24.2.x	NA	NA	NA
OCI Adaptor	24.2.1	NA	24.2.x	NA	NA	- 1.29.x - 1.28.x - 1.27.x	24.2.x	NA	NA	NA

Table 3-2 (Cont.) Compatibility Matrix

CNC NF	NF Version	CNE	cnDBTier	OSO	ASM S/W	Kubernetes	CNC Console	OCNADD	OCCM	OCI Adaptor
OCI Adaptor	24.2.0	NA	24.2.x	NA	NA	• 1.29.x • 1.28.x • 1.27.x	24.2.x	NA	NA	NA
OSO	24.2.5	NA	NA	NA	NA	• 1.29.x • 1.28.x • 1.27.x	NA	NA	NA	NA
OSO	24.2.0	NA	NA	NA	NA	• 1.29.x • 1.28.x • 1.27.x	NA	NA	NA	NA
Policy	24.2.6	• 25.1.1xx • 24.3.x • 24.2.x	• 24.2.x • 24.1.x • 23.4.x	• 24.2.x • 24.1.x • 23.4.x	1.14.6	• 1.31.x • 1.30.x • 1.29.x	24.2.x	25.1.1xx	24.2.x	NA
Policy	24.2.5	• 25.1.1xx • 24.3.x • 24.2.x	• 24.2.x • 24.1.x • 23.4.x	• 24.2.x • 24.1.x • 23.4.x	1.14.6	• 1.31.x • 1.30.x • 1.29.x	24.2.x	25.1.1xx	24.2.x	NA
Policy	24.2.4	• 25.1.1xx • 24.3.x • 24.2.x • 24.1.x • 23.4.x	• 24.2.x • 24.1.x • 23.4.x	• 24.2.x • 24.1.x • 23.4.x	1.14.6	• 1.31.x • 1.30.x • 1.29.x • 1.28.x • 1.27.x	24.2.x	25.1.1xx	24.2.x	NA

Table 3-2 (Cont.) Compatibility Matrix

CNC NF	NF Version	CNE	cnDBTier	OSO	ASM S/W	Kubernetes	CNC Console	OCNADD	OCCM	OCI Adaptor
Policy	24.2.3	• 24.2.x • 24.1.x • 23.4.x	• 24.2.x • 24.1.x • 23.4.x	• 24.2.x • 24.1.x • 23.4.x	1.14.6	• 1.29.x • 1.28.x • 1.27.x	24.2.x	NA	24.2.x	NA
Policy	24.2.2	• 24.2.x • 24.1.x • 23.4.x	• 24.2.x • 24.1.x • 23.4.x	• 24.2.x • 24.1.x • 23.4.x	1.14.6	• 1.29.x • 1.28.x • 1.27.x	24.2.x	NA	24.2.x	NA
Policy	24.2.1	• 24.2.x • 24.1.x • 23.4.x	• 24.2.x • 24.1.x • 23.4.x	• 24.2.x • 24.1.x • 23.4.x	1.14.6	• 1.29.x • 1.28.x • 1.27.x	24.2.x	NA	24.2.x	NA
Policy	24.2.0	• 24.2.x • 24.1.x • 23.4.x	• 24.2.x • 24.1.x • 23.4.x	• 24.2.x • 24.1.x • 23.4.x	1.14.6	• 1.29.x • 1.28.x • 1.27.x	24.2.x	NA	24.2.x	NA
SCP	24.2.4	• 24.2.x • 24.1.x • 23.4.x	• 24.2.x • 24.1.x • 23.4.x	• 24.2.x • 24.1.x • 23.4.x	• 1.14.6 • 1.11.8	• 1.29.x • 1.28.x • 1.27.x	24.2.x	24.2.x	24.2.x	24.2.x

Table 3-2 (Cont.) Compatibility Matrix

CNC NF	NF Version	CNE	cnDBTier	OSO	ASM S/W	Kubernetes	CNC Console	OCNADD	OCCM	OCI Adaptor
SCP	24.2.3	• 24.2.x • 24.1.x • 23.4.x	• 24.2.x • 24.1.x • 23.4.x	• 24.2.x • 24.1.x • 23.4.x	• 1.14.6 • 1.11.8	• 1.29.x • 1.28.x • 1.27.x	24.2.x	24.2.x	24.2.x	24.2.x
SCP	24.2.2	• 24.2.x • 24.1.x • 23.4.x	• 24.2.x • 24.1.x • 23.4.x	• 24.2.x • 24.1.x • 23.4.x	• 1.14.6 • 1.11.8	• 1.29.x • 1.28.x • 1.27.x	24.2.x	24.2.x	24.2.x	24.2.x
SCP	24.2.1	• 24.2.x • 24.1.x • 23.4.x	• 24.2.x • 24.1.x • 23.4.x	• 24.2.x • 24.1.x • 23.4.x	• 1.14.6 • 1.11.8	• 1.29.x • 1.28.x • 1.27.x	24.2.x	24.2.x	24.2.x	24.2.x
SCP	24.2.0	• 24.2.x • 24.1.x • 23.4.x	• 24.2.x • 24.1.x • 23.4.x	• 24.2.x • 24.1.x • 23.4.x	• 1.14.6 • 1.11.8	• 1.29.x • 1.28.x • 1.27.x	24.2.x	24.2.x	24.2.x	24.2.x
SEPP	24.2.4	• 24.2.x • 24.1.x • 23.4.x	• 24.2.x • 24.1.x • 23.4.x	• 24.2.x • 24.1.x • 23.4.x	1.14.6	• 1.29.x • 1.28.x • 1.27.x	24.2.x	24.2.x	24.2.x	24.2.x

Table 3-2 (Cont.) Compatibility Matrix

CNC NF	NF Version	CNE	cnDBTier	OSO	ASM S/W	Kubernetes	CNC Console	OCNADD	OCCM	OCI Adaptor
SEPP	24.2.3	• 24.2.x • 24.1.x • 23.4.x	• 24.2.x • 24.1.x • 23.4.x	• 24.2.x • 24.1.x • 23.4.x	1.14.6	• 1.29.x • 1.28.x • 1.27.x	24.2.x	24.2.x	24.2.x	24.2.x
SEPP	24.2.2	• 24.2.x • 24.1.x • 23.4.x	• 24.2.x • 24.1.x • 23.4.x	• 24.2.x • 24.1.x • 23.4.x	1.14.6	• 1.29.x • 1.28.x • 1.27.x	24.2.x	24.2.x	24.2.x	24.2.x
SEPP	24.2.1	• 24.2.x • 24.1.x • 23.4.x	• 24.2.x • 24.1.x • 23.4.x	• 24.2.x • 24.1.x • 23.4.x	1.14.6	• 1.29.x • 1.28.x • 1.27.x	24.2.x	24.2.x	24.2.x	24.2.x
SEPP	24.2.0	• 24.2.x • 24.1.x • 23.4.x	• 24.2.x • 24.1.x • 23.4.x	• 24.2.x • 24.1.x • 23.4.x	1.14.6	• 1.29.x • 1.28.x • 1.27.x	24.2.x	24.2.x	24.2.x	24.2.x
UDR	24.2.5	• 24.2.x • 24.1.x • 23.4.x	• 24.2.x • 24.1.x • 23.4.x	• 24.2.x • 24.1.x • 23.4.x	• 1.14.6 • 1.11.8	• 1.29.x • 1.28.x • 1.27.x	24.2.x	NA	24.2.x	NA

Table 3-2 (Cont.) Compatibility Matrix

CNC NF	NF Version	CNE	cnDBTier	OSO	ASM S/W	Kubernetes	CNC Console	OCNADD	OCCM	OCI Adaptor
UDR	24.2.4	• 24.2.x • 24.1.x • 23.4.x	• 24.2.x • 24.1.x • 23.4.x	• 24.2.x • 24.1.x • 23.4.x	• 1.14.6 • 1.11.8	• 1.29.x • 1.28.x • 1.27.x	24.2.x	NA	24.2.x	NA
UDR	24.2.3	• 24.2.x • 24.1.x • 23.4.x	• 24.2.x • 24.1.x • 23.4.x	• 24.2.x • 24.1.x • 23.4.x	• 1.14.6 • 1.11.8	• 1.29.x • 1.28.x • 1.27.x	24.2.x	NA	24.2.x	NA
UDR	24.2.2	• 24.2.x • 24.1.x • 23.4.x	• 24.2.x • 24.1.x • 23.4.x	• 24.2.x • 24.1.x • 23.4.x	• 1.14.6 • 1.11.8	• 1.29.x • 1.28.x • 1.27.x	24.2.x	NA	24.2.x	NA
UDR	24.2.1	• 24.2.x • 24.1.x • 23.4.x	• 24.2.x • 24.1.x • 23.4.x	• 24.2.x • 24.1.x • 23.4.x	• 1.14.6 • 1.11.8	• 1.29.x • 1.28.x • 1.27.x	24.2.x	NA	24.2.x	NA
UDR	24.2.0	• 24.2.x • 24.1.x • 23.4.x	• 24.2.x • 24.1.x • 23.4.x	• 24.2.x • 24.1.x • 23.4.x	• 1.14.6 • 1.11.8	• 1.29.x • 1.28.x • 1.27.x	24.2.x	NA	24.2.x	NA

3.3 3GPP Compatibility Matrix

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

Table 3-3 3GPP Compatibility Matrix

CNC NF	NF Version	3GPP
BSF	24.2.x	• 3GPP TS 23.501 v17.7.0 • 3GPP TS 23.501 v18.4 • 3GPP TS 23.502 v17.7 • 3GPP TS 23.502 v18.4 • 3GPP TS 23.503 V17.7 • 3GPP TS 23.503 V18.4 • 3GPP TS 29.500 v18.3.0 • 3GPP TS 29.500 v17.7.0 • 3GPP TS 29.510 v18.4 • 3GPP TS 29.510 v17.7 • 3GPP TS 29.513 V17.7 • 3GPP TS 29.513 V18.4 • 3GPP TS 29.521 v17.7.0 • 3GPP TS 29.521 v18.3.0 • 3GPP TS 33.501 V17.7.0 • 3GPP TS 33.501 V18.3.0
CNC Console	24.2.x	NA
cnDBTier	24.2.x	NA
CNE	24.2.x	NA
NEF	24.2.0	• 3GPP TS 29.338 v 17.1.0 • 3GPP TS 23.040 v 17.2.0 • 3GPP TS 29.122 v 16.10.0 , 17.10.0 • 3GPP TS 23.222 v 16.9.0 • 3GPP TS 23.501 v 16.10.0 • 3GPP TS 23.502 v 16.10.0 • 3GPP TS 29.514 v 16.10.0 • 3GPP TS 29.521 v 16.10 • 3GPP TS 29.503 v 16.14.0 • 3GPP TS 29.515 v 16.7 • 3GPP TS 29.222 v 16.5.0 • 3GPP TS 29.500 v 16.6.0 • 3GPP TS 29.501 v 16.6.0 • 3GPP TS 29.522 v 16.10.0, 17.10.0 • 3GPP TS 29.510 v 16.6.0 • 3GPP TS 29.591 v 16.3.0 • 3GPP TS 29.518 v 16.14.0 • 3GPP TS 33.501 v 17.7.0 • 3GPP TS 29.504 v 16.10.0 • 3GPP TS 29.519 v 16.11.0 • 3GPP TS 29.508 v 16.11.0 • 3GPP TS 23.682 v 16.9.0 • 3GPP TS 29.337 v 16.1.0 • 3GPP TS 29.214 v 16.7.0 • 3GPP TS 32.291 v16.14 • 3GPP TS 32.290 v16.10.0 • 3GPP TS 32.254 v16.6.0

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

CNC NF	NF Version	3GPP
NRF	24.2.x	• 3GPP TS 29.510 v15.5 • 3GPP TS 29.510 v16.3.0 • 3GPP TS 29.510 v16.7 • 3GPP TS 29.510 v17.7
NSSF	24.2.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
OCCM	24.2.x	• 3GPP TS 33.310-h30 • 3GPP TR 33.876 v.0.3.0
OSO	24.2.0	NA
Policy	24.2.x	• 3GPP TS 33.501 v17.7.0 • 3GPP TS 29.500v17.12.0 • 3GPP TS 23.501v17.10.0 • 3GPP TS 23.502v17.10.0 • 3GPP TS 23.503v17.10.0 • 3GPP TS 29.504v17.12.0 • 3GPP TS 29.507v17.10.0 • 3GPP TS 29.510v17.11.0 • 3GPP TS 29.512v17.12.0 • 3GPP TS 29.513v17.12.0 • 3GPP TS 29.514v17.09.0 • 3GPP TS 29.214v17.4.0 • 3GPP TS 29.518v17.12.0 • 3GPP TS 29.519v17.12.0 • 3GPP TS 29.520v17.11 • 3GPP TS 29.521v17.9.0 • 3GPP TS 29.525v17.9.0 • 3GPP TS 29.594v17.5.0 • 3GPP TS 23.203 v16.2.0 • 3GPP TS 29.212 V16.3.0 • 3GPP TS 29.213v16.3 • 3GPP TS 29.214 v16.2.0 • 3GPP TS 29.219 v16.0.0 • 3GPP TS 29.335v16.0
SCP	24.2.x	• 3GPP TS 29.500 R16 v16.6.0 • 3GPP TS 29.501 R16 v16.5.0
SEPP	24.2.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 29.573 v17.6.0 • 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 3-3 (Cont.) 3GPP Compatibility Matrix

CNC NF	NF Version	3GPP
UDR	24.2.x	• 3GPP TS 29.505 v15.4.0 • 3GPP TS 29.504 v16.2.0 • 3GPP TS 29.519 v16.2.0 • 3GPP TS 29.511 v17.2.0

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

3.4 Common Microservices Load Lineup

This section provides information about common microservices and ATS for the specific NF versions in Oracle Communications Cloud Native Core Release 3.24.2.

Table 3-4 Common Microservices Load Lineup for Network Functions

CNC NF	NF Version	Alternate Route Svc	App-Info	ASM Configuration	ATS Framework	Config-Server	Debug-tool	Egress Gateway	Ingress Gateway	Helm Test	Mediation	NRF-Client	Perf-Info
BSF	24.2.3	24.2.14	24.2.12	24.2.0	24.2.5	24.2.12	24.2.5	24.2.14	24.2.14	24.2.4	NA	24.2.7	24.2.12
BSF	24.2.2	24.2.10	24.2.9	24.2.0	24.2.4	24.2.9	24.2.3	24.2.10	24.2.10	24.2.3	NA	24.2.4	24.2.9
BSF	24.2.1	24.2.6	24.2.4	24.2.0	24.2.2	24.2.4	24.2.1	24.2.6	24.2.6	24.2.1	NA	24.2.2	24.2.4
BSF	24.2.0	24.2.5	24.2.2	24.2.0	24.2.0	24.2.2	24.2.1	24.2.5	24.2.5	24.2.1	NA	24.2.1	24.2.2
CNC Console	24.2.4	NA	NA	NA	NA	NA	24.2.5	NA	24.2.14	24.2.4	NA	NA	NA
CNC Console	24.2.3	NA	NA	NA	NA	NA	24.2.5	NA	24.2.13	24.2.4	NA	NA	NA
CNC Console	24.2.2	NA	NA	NA	NA	NA	24.2.3	NA	24.2.11	24.2.3	NA	NA	NA
CNC Console	24.2.1	NA	NA	NA	NA	NA	24.2.2	NA	24.2.8	24.2.2	NA	NA	NA
CNC Console	24.2.0	NA	NA	NA	NA	NA	24.2.1	NA	24.2.4	24.2.1	NA	NA	NA
NEF	24.2.0	NA	24.2.1	NA	24.2.2	24.2.1	24.2.1	24.2.4	24.2.4	24.2.1	NA	24.2.1	24.2.1
NRF	24.2.4	24.2.13	24.2.11	24.2.0	24.2.5	NA	24.2.4	24.2.13	24.2.13	24.2.4	NA	NA	24.2.11
NRF	24.2.3	24.2.11	24.2.8	24.2.0	24.2.4	NA	24.2.3	24.2.11	24.2.11	24.2.3	NA	NA	24.2.8

Table 3-4 (Cont.) Common Microservices Load Lineup for Network Functions

CNC NF	NF Version	Alternate Route Svc	App-Info	ASM Configuration	ATS Framework	Config-Server	Debug-tool	Egress Gateway	Ingress Gateway	Helm Test	Mediation	NRF-Client	Perf-Info
NRF	24.2.2	24.2.7	24.2.5	24.2.0	24.2.3	NA	24.2.2	24.2.7	24.2.7	24.2.2	NA	NA	24.2.5
NRF	24.2.1	24.2.5	24.2.1	24.2.0	24.2.2	NA	24.2.1	24.2.5	24.2.5	24.2.1	NA	NA	24.2.1
NRF	24.2.0	24.2.5	24.2.1	24.2.0	24.2.2	NA	24.2.1	24.2.5	24.2.5	24.2.1	NA	NA	24.2.1
NSSF	24.2.1	24.2.7	24.2.5	24.2.0	24.2.3	24.2.5	24.2.2	24.2.7	24.2.7	24.2.1	NA	24.2.3	24.2.5
NSSF	24.2.0	24.2.4	24.2.1	24.2.0	24.2.2	24.2.1	24.2.1	24.2.4	24.2.4	24.2.1	NA	24.2.1	24.2.1
OCCM	24.2.3	NA	NA	NA	NA	NA	24.2.5	NA	NA	24.2.4	NA	NA	NA
OCCM	24.2.2	NA	NA	NA	NA	NA	24.2.3	NA	NA	24.2.3	NA	NA	NA
OCCM	24.2.1	NA	NA	NA	NA	NA	24.2.2	NA	NA	24.2.2	NA	NA	NA
OCCM	24.2.0	NA	NA	NA	NA	NA	24.2.1	NA	NA	24.2.1	NA	NA	NA
Policy	24.2.6	24.2.14	24.2.14	24.2.0	24.2.5	24.2.14	24.2.5	24.2.14	24.2.14	24.2.4	NA	24.2.7	24.2.14
Policy	24.2.5	24.2.14	24.2.12	24.2.0	24.2.5	24.2.12	24.2.5	24.2.14	24.2.14	24.2.4	NA	24.2.7	24.2.12
Policy	24.2.4	24.2.14	24.2.10	24.2.0	24.2.4	24.2.10	24.2.3	24.2.12	24.2.12	24.2.3	NA	24.2.6	24.2.10
Policy	24.2.3	24.2.10	24.2.9	24.2.0	24.2.4	24.2.9	24.2.3	24.2.10	24.2.10	24.2.3	NA	24.2.4	24.2.9
Policy	24.2.2	24.2.6	24.2.4	24.2.0	24.2.2	24.2.4	24.2.1	24.2.6	24.2.6	24.2.1	NA	24.2.2	24.2.4
Policy	24.2.1	24.2.6	24.2.4	24.2.0	24.2.2	24.2.4	24.2.1	24.2.6	24.2.6	24.2.1	NA	24.2.2	24.2.4
Policy	24.2.0	24.2.5	24.2.2	24.2.0	24.2.0	24.2.2	24.2.1	24.2.5	24.2.5	24.2.1	NA	24.2.1	24.2.2
SCP	24.2.4	NA	NA	24.2.0	24.2.5	NA	24.2.5	NA	NA	24.2.4	24.2.5	NA	NA
SCP	24.2.3	NA	NA	24.2.0	24.2.4	NA	24.2.3	NA	NA	24.2.3`	24.2.4	NA	NA
SCP	24.2.2	NA	NA	24.2.0	24.2.3	NA	24.2.2	NA	NA	24.2.2	24.2.3	NA	NA
SCP	24.2.1	NA	NA	24.2.0	24.2.2	NA	24.2.1	NA	NA	24.2.1	24.2.2	NA	NA
SCP	24.2.0	NA	NA	24.2.0	24.2.2	NA	24.2.1	NA	NA	24.2.1	24.2.2	NA	NA
SEPP	24.2.4	24.2.13	24.2.11	24.2.4	24.2.4	24.2.11	24.2.4	24.2.13	24.2.13	24.2.4	24.2.5	24.2.7	24.2.11
SEPP	24.2.3	24.2.11	24.2.8	24.2.3	24.2.3	24.2.8	24.2.3	24.2.11	24.2.11	24.2.3	24.2.4	24.2.4	24.2.8
SEPP	24.2.2	24.2.7	24.2.5	24.2.1	24.2.3	24.2.5	24.2.2	24.2.7	24.2.7	24.2.2	24.2.3	24.2.3	24.2.5
SEPP	24.2.1	24.2.7	24.2.5	24.2.1	24.2.3	24.2.5	24.2.2	24.2.7	24.2.7	24.2.2	24.2.3	24.2.3	24.2.5
SEPP	24.2.0	24.2.4	24.2.1	24.2.0	24.2.1	NA	24.2.1	24.2.4	24.2.4	24.2.1	24.2.2	24.2.1	24.2.1
UDR	24.2.5	24.2.14	24.2.11	24.2.0	24.2.5	24.2.11	24.2.5	24.2.14	24.2.14	24.2.4	NA	24.2.7	24.2.11
UDR	24.2.4	24.2.14	24.2.11	24.2.0	24.2.5	24.2.11	24.2.5	24.2.14	24.2.14	24.2.4	NA	24.2.7	24.2.11
UDR	24.2.3	24.2.11	24.2.8	24.2.0	24.2.4	24.2.8	24.2.3	24.2.11	24.2.11	24.2.3	NA	24.2.4	24.2.8
UDR	24.2.2	24.2.7	24.2.5	24.2.0	24.2.3	24.2.5	24.2.2	24.2.7	24.2.7	24.2.2	NA	24.2.3	24.2.5
UDR	24.2.1	24.2.7	24.2.5	24.2.0	24.2.3	24.2.5	24.2.2	24.2.7	24.2.7	24.2.2	NA	24.2.3	24.2.5
UDR	24.2.0	24.2.5	24.2.1	24.2.0	24.2.2	24.2.1	24.2.1	24.2.5	24.2.5	24.2.1	NA	24.2.1	24.2.1

3.5 Security Certification Declaration

This section lists the security tests and the corresponding dates of compliance for each network function:

3.5.1 BSF Security Certification Declaration

Release 24.2.3

Table 3-5 BSF Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	Apr 14, 2025	No unmitigated critical or high findings
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	Apr 7, 2025	No unmitigated critical or high findings
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	Apr 25, 2025	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	Apr 25, 2025	No findings

Overall Summary: No critical or severity 1 security issues were found during internal security testing.

Release 24.2.2

Table 3-6 BSF Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	Jan 21, 2025	No unmitigated critical or high findings
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	Jan 8, 2025	No unmitigated critical or high findings
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	Jan 23, 2025	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	Jan 27, 2025	No findings

Overall Summary: No critical or severity 1 security issues were found during internal security testing.

Release 24.2.1

Table 3-7 BSF Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	Oct 2, 2024	No unmitigated critical or high findings

Table 3-7 (Cont.) BSF Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	Sep 2, 2024	No unmitigated critical or high findings
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	Oct 2, 2024	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	Oct 4, 2024	No findings

Overall Summary: No critical or severity 1 security issues were found during internal security testing.

Release 24.2.0

Table 3-8 BSF Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	July 19, 2024	No unmitigated critical or high findings
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	July 11, 2024	No unmitigated critical or high findings

Table 3-8 (Cont.) BSF Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	July 17, 2024	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	Aug 02, 2024	No findings

Overall Summary: No critical or severity 1 security issues were found during internal security testing.

3.5.2 CNC Console Security Certification Declaration

Release 24.2.4

Table 3-9 CNC Console Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	Apr 23, 2025	No unmitigated critical or high findings
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	Jan 13, 2025	No unmitigated critical or high findings
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	Apr 23, 2025	No unmitigated critical or high finding

Table 3-9 (Cont.) CNC Console Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	Apr 23, 2025	No findings

Overall Summary: No critical or severity 1 security issues were found during internal security testing.

Release 24.2.3

Table 3-10 CNC Console Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	Apr 11, 2025	No unmitigated critical or high findings
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	Jan 13, 2025	No unmitigated critical or high findings
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	Apr 11, 2025	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	Apr 11, 2025	No findings

Overall Summary: No critical or severity 1 security issues were found during internal security testing.

Release 24.2.2

Table 3-11 CNC Console Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	Jan 13, 2025	No unmitigated critical or high findings
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	Jan 13, 2025	No unmitigated critical or high findings
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	Jan 13, 2025	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	Jan 13, 2025	No findings

Overall Summary: No critical or severity 1 security issues were found during internal security testing.

Release 24.2.1

Table 3-12 CNC Console Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	Oct 23, 2024	No unmitigated critical or high findings

Table 3-12 (Cont.) CNC Console Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	Oct 24, 2024	No unmitigated critical or high findings
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	Oct 23, 2024	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	Oct 23, 2024	No findings

Overall Summary: No critical or severity 1 security issues were found during internal security testing.

Release 24.2.0

Table 3-13 CNC Console Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	July 9, 2024	No unmitigated critical or high findings
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	July 9, 2024	No unmitigated critical or high findings

Table 3-13 (Cont.) CNC Console Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	July 9, 2024	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	July 9, 2024	No findings

Overall Summary: No critical or severity 1 security issues were found during internal security testing.

3.5.3 NEF Security Certification Declaration

Release 24.2.0

Table 3-14 NEF Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	June 13, 2024	No unmitigated critical or high findings
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	May 20, 2024	No unmitigated critical or high findings
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	June 13, 2024	No unmitigated critical or high finding

Table 3-14 (Cont.) NEF Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	June 13, 2024	No findings

Overall Summary: No critical or severity 1 security issues were found during internal security testing.

3.5.4 NRF Security Certification Declaration

Release 24.2.4

Table 3-15 NRF Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	April 2, 2025	No unmitigated critical or high findings
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	April 2, 2025	No unmitigated critical or high findings
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	April 2, 2025	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	April 2, 2025	No findings

Overall Summary: No critical or severity 1 security issues were found during internal security testing.

Release 24.2.3

Table 3-16 NRF Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	January 7, 2025	No unmitigated critical or high findings
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	January 7, 2025	No unmitigated critical or high findings
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	January 7, 2025	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	January 7, 2025	No findings

Overall Summary: No critical or severity 1 security issues were found during internal security testing.

Release 24.2.2

Table 3-17 NRF Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	October 25, 2024	No unmitigated critical or high findings

Table 3-17 (Cont.) NRF Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	October 25, 2024	No unmitigated critical or high findings
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	October 25, 2024	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	October 25, 2024	No findings

Overall Summary: No critical or severity 1 security issues were found during internal security testing.

Release 24.2.1

Table 3-18 NRF Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	September 13, 2024	No unmitigated critical or high findings
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	September 13, 2024	No unmitigated critical or high findings

Table 3-18 (Cont.) NRF Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	September 13, 2024	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	September 13, 2024	No findings

Overall Summary: No critical or severity 1 security issues were found during internal security testing.

Release 24.2.0

Table 3-19 NRF Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	July 24, 2024	No unmitigated critical or high findings
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	July 24, 2024	No unmitigated critical or high findings
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	July 24, 2024	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	July 24, 2024	No findings

Overall Summary: No critical or severity 1 security issues were found during internal security testing.

3.5.5 NSSF Security Certification Declaration

Release 24.2.1

Table 3-20 NSSF Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	October 11, 2024	No unmitigated critical or high findings
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	October 11, 2024	No unmitigated critical or high findings
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	October 11, 2024	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	October 11, 2024	No findings

Release 24.2.0

Table 3-21 NSSF Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	June 3, 2024	No unmitigated critical or high findings

Table 3-21 (Cont.) NSSF Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	June 3, 2024	No unmitigated critical or high findings
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	June 3, 2024	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	June 3, 2024	No findings

Overall Summary: No critical or severity 1 security issues were found during internal security testing.

3.5.6 OCCM Security Certification Declaration

Release 24.2.3

Table 3-22 OCCM Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	Apr 10, 2025	No unmitigated critical or high findings
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	Oct 17, 2024	No unmitigated critical or high findings

Table 3-22 (Cont.) OCCM Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	Apr 10, 2025	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	Apr 10, 2025	No findings

Overall Summary: No critical or severity 1 security issues were found during internal security testing.

Release 24.2.2

Table 3-23 OCCM Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	January 10, 2025	No unmitigated critical or high findings
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	Oct 17, 2024	No unmitigated critical or high findings
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	January 10, 2025	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	January 10, 2025	No findings

Overall Summary: No critical or severity 1 security issues were found during internal security testing.

Release 24.2.1

Table 3-24 OCCM Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	July 5, 2024	No unmitigated critical or high findings
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	Oct 17, 2024	No unmitigated critical or high findings
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	Oct 17, 2024	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	Oct 17, 2024	No findings

Overall Summary: No critical or severity 1 security issues were found during internal security testing.

Release 24.2.0

Table 3-25 OCCM Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	July 5, 2024	No unmitigated critical or high findings

Table 3-25 (Cont.) OCCM Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	July 5, 2024	No unmitigated critical or high findings
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	July 5, 2024	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	July 5, 2024	No findings

Overall Summary: No critical or severity 1 security issues were found during internal security testing.

3.5.7 Policy Security Certification Declaration

Policy 24.2.6

Table 3-26 Policy Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	June 4, 2025	No unmitigated critical or high findings
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	April 7, 2025	No unmitigated critical or high findings

Table 3-26 (Cont.) Policy Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	June 4, 2025	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	June 9, 2025	No findings

Overall Summary: No critical or severity 1 security issues were found during internal security testing.

Policy 24.2.5

Table 3-27 Policy Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	April 14, 2025	No unmitigated critical or high findings
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	April 7, 2025	No unmitigated critical or high findings
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	April 25, 2025	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	April 25, 2025	No findings

Overall Summary: No critical or severity 1 security issues were found during internal security testing.

Policy 24.2.4

Table 3-28 Policy Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	March 11, 2025	No unmitigated critical or high findings
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	Ferbruary 26, 2025	No unmitigated critical or high findings
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	March 11, 2025	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	March 12, 2025	No findings

Overall Summary: No critical or severity 1 security issues were found during internal security testing.

Policy 24.2.3

Table 3-29 Policy Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	January 21, 2025	No unmitigated critical or high findings

Table 3-29 (Cont.) Policy Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	January 8, 2025	No unmitigated critical or high findings
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	January 23, 2025	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	January 27, 2025	No findings

Overall Summary: No critical or severity 1 security issues were found during internal security testing.

Policy 24.2.2

Table 3-30 Policy Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	October 2, 2024	No unmitigated critical or high findings
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	September 10, 2024	No unmitigated critical or high findings

Table 3-30 (Cont.) Policy Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	October 2, 2024	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	November 5, 2024	No findings

Overall Summary: No critical or severity 1 security issues were found during internal security testing.

Policy 24.2.1

Table 3-31 Policy Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	October 2, 2024	No unmitigated critical or high findings
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	September 10, 2024	No unmitigated critical or high findings
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	October 2, 2024	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	October 4, 2024	No findings

Overall Summary: No critical or severity 1 security issues were found during internal security testing.

Policy 24.2.0

Table 3-32 Policy Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	July 19, 2024	No unmitigated critical or high findings
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	July 9, 2024	No unmitigated critical or high findings
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	July 17, 2024	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	August 02, 2024	No findings

Overall Summary: No critical or severity 1 security issues were found during internal security testing.

3.5.8 SCP Security Certification Declaration

SCP 24.2.4

Table 3-33 SCP Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	April 15, 2025	No unmitigated critical or high findings
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	April 15, 2025	No unmitigated critical or high findings
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	April 15, 2025	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	April 15, 2025	No findings

SCP 24.2.3

Table 3-34 SCP Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	January 30, 2025	No unmitigated critical or high findings

Table 3-34 (Cont.) SCP Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	January 30, 2025	No unmitigated critical or high findings
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	January 30, 2025	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	January 30, 2025	No findings

SCP 24.2.2

Table 3-35 SCP Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	October 24, 2024	No unmitigated critical or high findings
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	October 24, 2024	No unmitigated critical or high findings
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	October 24, 2024	No unmitigated critical or high finding

Table 3-35 (Cont.) SCP Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	October 24, 2024	No findings

SCP 24.2.1

Table 3-36 SCP Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	September 19, 2024	No unmitigated critical or high findings
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	September 19, 2024	No unmitigated critical or high findings
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	September 19, 2024	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	September 19, 2024	No findings

Overall Summary: No critical or severity 1 security issues were found or pending during internal security testing.

SCP 24.2.0

Table 3-37 SCP Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	July 5, 2024	No unmitigated critical or high findings
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	July 5, 2024	No unmitigated critical or high findings
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	July 5, 2024	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	July 5, 2024	No findings

Overall Summary: No critical or severity 1 security issues were found or pending during internal security testing.

3.5.9 SEPP Security Certification Declaration

Release 24.2.4

Table 3-38 SEPP Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	April 18, 2025	NA

Table 3-38 (Cont.) SEPP Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	NA	NA
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	April 18, 2025	NA
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	April 18, 2025	No issues found. Scan done through McAfee.

Overall Summary: No critical or severity 1 security issues were found during internal security testing.

Release 24.2.3

Table 3-39 SEPP Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	Jan 15, 2025	NA
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	NA	NA

Table 3-39 (Cont.) SEPP Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	Jan 8, 2025	NA
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	Jan 16, 2025	No issues found. Scan done through McAfee.

Overall Summary: No critical or severity 1 security issues were found during internal security testing.

Release 24.2.2

Table 3-40 SEPP Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	NA	NA
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	NA	NA
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	NA	NA
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	Dec 30, 2024	No issues found. Scan done through McAfee.

Overall Summary: No critical or severity 1 security issues were found during internal security testing.

Release 24.2.1

Table 3-41   SEPP Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	Oct 24, 2024	No unmitigated critical or high findings. Scan done through Fortify.
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	NA	No unmitigated critical, high, medium, and low findings. Scan done through RestFuzz.
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	Oct 25, 2024	No unmitigated critical or high findings. Scan done through Blackduck.
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	Oct 25, 2024	No issues found. Scan done through McAfee.

Overall Summary: No critical or severity 1 security issues were found during internal security testing.

Release 24.2.0

Table 3-42   SEPP Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	July 05, 2024	No unmitigated critical or high findings. Scan done through Fortify.

Table 3-42 (Cont.) SEPP Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	July 05, 2024	No unmitigated critical, high, medium, and low findings. Scan done through RestFuzz.
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	July 05, 2024	No unmitigated critical or high findings. Scan done through Blackduck.
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	July 05, 2024	No issues found. Scan done through McAfee.

Overall Summary: No critical or severity 1 security issues were found during internal security testing.

3.5.10 UDR Security Certification Declaration

Release 24.2.5

Table 3-43 UDR Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	Jan 16, 2025	No unmitigated critical or high findings
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	April 16, 2025	No unmitigated critical or high findings

Table 3-43 (Cont.) UDR Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	April 16, 2025	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	April 16, 2025	No findings

Release 24.2.4

Table 3-44 UDR Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	Jan 16, 2025	No unmitigated critical or high findings
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	April 16, 2025	No unmitigated critical or high findings
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	April 16, 2025	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	April 16, 2025	No findings

Overall Summary: No critical or severity 1 security issues were found during internal security testing.

Release 24.2.3

Table 3-45 UDR Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	Jan 16, 2025	No unmitigated critical or high findings
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	Jan 16, 2025	No unmitigated critical or high findings
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	Jan 16, 2025	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	Jan 16, 2025	No findings

Overall Summary: No critical or severity 1 security issues were found during internal security testing.

Release 24.2.2

Table 3-46 UDR Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	October 24, 2024	No unmitigated critical or high findings

Table 3-46 (Cont.) UDR Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	October 24, 2024	No unmitigated critical or high findings
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	October 24, 2024	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	October 24, 2024	No findings

Overall Summary: No critical or severity 1 security issues were found during internal security testing.

Release 24.2.1

Table 3-47 UDR Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	October 24, 2024	No unmitigated critical or high findings
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	October 24, 2024	No unmitigated critical or high findings

Table 3-47 (Cont.) UDR Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	October 24, 2024	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	October 24, 2024	No findings

Overall Summary: No critical or severity 1 security issues were found during internal security testing.

Release 24.2.0

Table 3-48 UDR Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	July 5, 2024	No unmitigated critical or high findings
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	July 5, 2024	No unmitigated critical or high findings
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	July 5, 2024	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	July 5, 2024	No findings

Overall Summary: No critical or severity 1 security issues were found during internal security testing.

3.6 Documentation Pack

All documents for Oracle Communications Cloud Native Core (CNC) 3.24.2 are available for download on SecureSites and MOS.

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

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

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

4

Resolved and Known Bugs

This chapter lists the resolved and known bugs for Oracle Communications Cloud Native Core release 3.24.2.

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

4.1 Severity Definitions

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

Severity 1

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

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

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

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

Severity 2

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

Severity 3

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

Severity 4

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

4.2 Resolved Bug List

The following Resolved Bugs tables list the bugs that are resolved in Oracle Communications Cloud Native Core Release 3.24.2.

4.2.1 BSF Resolved Bugs

BSF 24.2.3 Resolved Bugs

There are no new resolved bugs in this release.

Table 4-1   BSF 24.2.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37291922	Post BSF upgrade Over load congestion kicked in	High CPU utilization was observed when BSF was upgraded to 23.4.4.	1	23.4.4
37385289	When leader diam-gateway pod goes down, stale entries in distributed cache causes IPR to fail due to NPEs	When the Diameter Gateway leader pod went down, the entries remained stale in distributed cache. But, while iterating through those entries for inter-pod routing, Diameter Gateway worked in Network Processing Engine (NPE). This caused message routing failure.	2	23.4.6
37440298	Case-sensitive name for diameter-identity is causing voice call failure with "No peer to send REQ" error during IPR	When peer identity was stored in the peerInfo cache, it was stored in the cache after converting to lowercase. With new *IPRLocalPeerTable* changes, the query to *IPRLocalPeerTable* was not changing destination host to lowercase causing failure in finding alternate Diameter Gateway peer to route the message.	3	23.4.6
37387650	BSF generating SYSTEM_OPERATIONAL_STATE_NORMAL alert	If the system was running in normal state, then SYSTEM_OPERATIONAL_STATE_NORMAL alert was getting triggered but not being cleared.	3	24.2.1
37301210	Duplicate bindng makes AAR fail with 5012 DIAMETER_UNABLE_TO_COMPLY	AAR was failing with 5012 DIAMETER_UNABLE_TO_COMPLY error due to duplicate binding.	3	24.2.0

Table 4-2 BSF ATS 24.2.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37312051	Perfinfo_Overload_Manager scenario is failing	"Perfinfo_Overload_Manager" scenario from Regression suite was failing.	3	24.2.1

Table 4-3 BSF 24.2.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36912417	BSF Management error handling feature is failing due to a missing validation when loading up new configurations	The error handling configurations topic name, *public.bsf.error.handler.config*, was same in bsf-mgmt and diam-gateway service. The only way to differentiate them was to use the service name, but service name based validation was missing, resulting in reading wrong configuration (from different service).	3	24.2.0

Table 4-4 BSF 24.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36415688	BSF Network Policy issue for Egress Gateway flows	Network Policy on BSF blocked the Egress Gateway flows.	3	23.4.0
36576036	BSF Missing Network Policy for Egress Prometheus & alert manager flows	In BSF custom values file, the path to Prometheus and alert manager did not contain the matching Network Policy.	3	23.4.0
36804359	False Alert: SCP_PEER_SET_UNAVAILABLE	`SCP_PEER_SET_UNAVAILABLE` alert was falsely triggered as `ocbsf_oc_egressgateway_peer_available_count` was returning multiple results per diameter gateway pod. An aggregation operator like min or max must be used in the expression to evaluate the actual value.	3	23.2.0

Table 4-4 (Cont.) BSF 24.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36612887	Diameter Alternate routing done with same Destination-Host	There were issues with rewriting the Destination-Host AVP when retrying to the alternate destination.	3	23.4.0
36621980	BSF Alerts Rule File caused 60 new alerts	BSF Alerts Rule file caused generation of 60 new alerts in Prometheus server.	3	23.2.4
36417329	BSF binding response adding "null" response for sd	BSF binding response to PCF included "null" response for `sd` parameter when setting up binding session.	4	23.2.0

4.2.2 CNC Console Resolved Bugs

Table 4-5 CNC Console 24.2.4 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37674867	Remote CNCC 24.2.2 install not able to load PCF SM Sub Policy but local CNCC 24.1.0 can	The user encountered a 400 Bad Request error, and the Policy Installa_Session_Rule screen failed to load because of double forward slashes (//) in the request URL.	3	24.2.2

Note:

Resolved bugs from 23.4.4, 24.1.1, and 24.2.3 have been forward ported to Release 24.2.4.

Table 4-6 CNC Console 24.2.3 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37802775	Improvements in CNCC upgrade/rollback procedure	The CNC Console upgrade and rollback procedure needed updates to improve clarity and ensure a better understanding of the process.	3	25.1.100

Table 4-6 (Cont.) CNC Console 24.2.3 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37802480	CNCC 24.3.0 Metric not displayed for one of the A-CNCC Query due to duplicate RefId	The CNC Console metric dashboard file had a duplicate Reference ID. The dashboard file has to be updated to remove the duplicate Reference ID, making each entry unique.	3	24.3.0
37802598	Wrong MIB file not corresponding SNMP-Notifier sent info in the alert trap towards SNMP server	The wrong MIB file, which did not correspond to the SNMP-Notifier, was sent in the alert trap towards the SNMP server.	3	24.2.0

Note:

Resolved bugs from 23.4.4 and 24.1.1 have been forward ported to Release 24.2.3.

Table 4-7 CNC Console 24.2.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37471486	DBTier replication is down after CNCC upgrade	After the CNC Console upgrade, cnDBTier replication was down. Replication was failing due to DML and DDL commands being executed out of order on replicated sites.	2	23.2.1
37372664	Route Path exceeding length for GW metrics after upgrade to 24.2.1	The length for Route_path in CNCC metrics exceeded the limit, causing the OSO prom-svr to crash after CNCC upgrade.	2	24.2.0

Table 4-7 (Cont.) CNC Console 24.2.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37335886	CNCC 24.2.1 Installation guide documentation queries	• The note "If cnDBTier version starting from 23.2.x onwards is used during the deployment, set the `ndb_allow_copying_alter_table` parameter to 'ON' in the `occncc_dbtier__custom_values_.yaml` file before installing CNC Console" had to be updated in the 'Configuring Database' section of *Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide.* • A note had to be added to update default namespace to CNC Console deployed namespace in the CNC Console Alert configuration in Prometheus section of *Oracle Communications Cloud Native Configuration Console User Guide.*	3	24.2.1

Note:

Resolved bugs from 23.4.3 and 24.1.1 have been forward ported to release 24.2.2.

Table 4-8 CNC Console 24.2.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36918008	High Memory usage observed with mcore-ingress-gateway pod and the logs showing "java.lang.OutOfMemory Error"	High memory usage was observed in mcore-ingress-gateway pod.	2	24.1.0
36950084	Issue enabling IAM Keycloak logs	There was an issue in enabling IAM Keycloak logs. Log Level is changed to debug by default for event logging.	3	23.4.1
37102681	Changing settings for the IAM admin user via REST API	The user could not change the admin user settings on CNC IAM Console using REST API.	3	23.4.0
37043384	OSO prom-svr crashing after CS-AMPCF/DB/CNCC upgrade to 23.4.x	OSO prom-svr stopped working after CS-AMPCF/DB/CNC Console upgrade to 23.4.x.	3	23.4.0
37175346	IAM GUI cannot delete User Credentials	The user was not able to delete the credentials entry from IAM GUI.	4	24.2.0

Table 4-9 CNC Console 24.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36752027	During in solution upgrade of NEF in a 2 site GR setup, while upgrading CNCC from 24.1.0 to 24.2.0 rc2, CNDB replication is broken	cnDBTier replication broke when there was traffic on cnDBTier during CNC Console upgrade. As a resolution, CNC Console IAM DB schema was updated.	2	24.2.0
36738843	CNCC PDB ALLOWED DISRUPTIONS 0 - Kubernetes Upgrade fail	The `podDisruptionBudget` configuration had the incorrect value.	3	24.1.0
36618217	LDAP integration failing due to "manage DSA IT" request from CNCC iam-kc	CNC Console was unable to integrate with LDAP because of a "Manage DSA IT" request from CNC Console iam-kc.	3	24.2.0

Table 4-9 (Cont.) CNC Console 24.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36603448	Data Director Instance Configuration Examples are incorrect	The CNC Console instance configuration examples for Data Director had the incorrect service name for the Data Director API.	4	24.1.0

> **Note:**
>
> Resolved bugs from 23.4.1 and 23.4.2 have been forward ported to Release 24.2.0.

4.2.3 cnDBTier Resolved Bugs

Table 4-10 cnDBTier 24.2.5 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37883263	`dbtscale_vertical_pvc` failing for ndbmgmd, ndbmysqld, ndbappmysqld, and ndbmtd	`dbtscale_vertical_pvc` script contains a variable which can be configured for PVC size in the db-replication-svc deployment called "GEO_RECOVERY_RESOURCES_DISK_SIZE". However, this variable was not present in the db-replication-svc deployment in release 24.2.5. Hence, dbtscale_vertical_pvc script was failing for ndbmgmd, ndbmysqld, ndbappmysqld, and ndbmtd pods.	2	24.2.5
37807135	The `dbtscale_ndbmtd_pods` script was not working in release 24.2.5	`dbtscale_ndbmtd_pods` was failing in single-site setup of 24.2.5 as the labels were not present in stateful sets (STS).	2	24.2.4
37642018	`dbtscale_vertical_pvc` script was not working on single-site setup	During a single-site deployment, `dbtscale_vertical_pvc` script was failing due to missing Container command.	2	25.1.100

Table 4-10 (Cont.) cnDBTier 24.2.5 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37655902	While upgrading using `dbtscale_vertical_pvc` script, the script was failing at the upgrade phase	While upgrading cnDBTier using `dbtscale_vertical_pvc` script, the script was failing due to timeout issue while restarting pods on MySQL NDB cluster.	2	25.1.100
37789389	`dbtscale_vertical_pvc` script was not working if `ndbdisksize` was in decimal format	`dbtscale_vertical_pvc` script was failing when `ndbdisksize` value was in decimal format.	3	23.3.1
37649201	Upgrade was failing with an error `serviceaccount "mysql-cluster-upgrade-serviceaccount" not found` although the upgrade service account was existing	If there was an existing upgrade service account that was created during Helm installation, and in the `custom_values.yaml` file, if the `mysql-cluster-upgrade-serviceaccount` parameter was set to false, then the upgrade failed with the following error message. `serviceaccount "mysql-cluster-upgrade-serviceaccount" not found`	3	24.2.2
37663827	Automatic login to remote server from replication service pod was not working due to remote server private key permission issue	When the remote server private SSH key was set to 644, the automatic login to remote server from the replication service pod was not working. To clear this, the remote server SSH key permission was set to 600 in the Dockerfile.	3	24.4.6
37622137	On a prefix-enabled 3-channel setup, Disaster Recovery was stalling for a non-fatal scenario	On a prefix-enabled 3-channel setup, Disaster Recovery was stalling for a non-fatal scenario. `db-replication-svc` was shutting down all SQL pods before geo redundant replication proceeded with NDB_RESTORE. This led to an accumulating queue of shutdown tasks, eventually causing the service to stall.	3	25.1.100

Table 4-10 (Cont.) cnDBTier 24.2.5 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37761092	Update the workaround for GRR stuck in RECONNECTSQLNODES	While performing disaster recovery on a 2-site 3-channel setup for a non-fatal scenario, the script was stalling at RECONNECTSQLNODES state during Geo-redundant Replication (GRR), It was required to restart the replication svc pod for GRR to proceed.	3	24.2.4
37753846	Vertical scaling of PVC was failing while using `dbtscale_vertical_pvc` script	During vertical scaling of Persistent Volume Claim (PVC), the `dbtscale_vertical_pvc` script was failing as `DBTIER_RELEASE_NAME` was not configured.	3	24.2.4
37875671	`dbtscale_vertical_pvc` script was not working when re-executed	On a single-site setup deployment, dbtscale_vertical_pvc script was run with a wrong file path for the Helm chart due to which the script was unsuccessful. However, the script was then re-executed with the correct path but, ndbmysqld stateful sets were deleted in the previous run and hence, the script failed again.	3	24.2.5

Table 4-11 cnDBTier 24.2.4 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37468403	Cluster Failure observed in PCF microservices	Clusters failed in PCF microservices during MySQL cluster recovery. This issue is resolved by improving the MySQL cluster node recovery logic.	1	23.4.4
37447839	While upgrading the PVC value on 25.1.100-rc.2 dbtscale_vertical_pvc script is getting failed	The `dbtscale_vertical_pvc` script failed due to incorrect version number.	2	25.1.100
37404406	DBTier 24.2.1 helm rollback from TLS to non-TLS same version not dropping TLS	Rollback from a TLS enabled version to a non-TLS version failed.	3	24.2.1
37365660	cnDBtier 24.2.2 restore database from backup is not restoring the data completely	The `cndbtier_restore.sh` script did not restore the data completely.	3	24.2.2

Table 4-11 (Cont.) cnDBTier 24.2.4 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37448493	Seg. fault observed with ndbmtd while dbtpasswd change in progress	Segmentation fault was observed in the `ndbmtd` pods when cnDBTier password change was in progress.	3	25.1.100
37526391	Crash observed in data nodes during Installation	Data nodes crashed during installation due to segmentation fault in the `ndbmtd` pods when cnDBTier password change was in progress.	3	25.1.100
37527057	MTD pods restarted during upgrade from 23.4.2 to 25.1.100	MTD pods restarted during upgrade due to segmentation fault in the `ndbmtd` pods when cnDBTier password change was in progress.	3	25.1.100
37601066	cnDBTier:24.2.x:snmp MIB Complain from SNMP server	cnDBTier SNMP MIB file did not support appending *.1* in the OID value.	3	24.2.0
37550094	In Installation Guide at traffic Segregation with CNLB need to change siteport 80 to 8080	The port configuration to setup traffic segregation with CNLB was incorrect for the replication service.	4	24.3.0

Table 4-12 cnDBTier 24.2.3 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37214770	Standby replication channel went into FAILED state and didn't recover after restarting one management Dell switch	When adding a site, the system did not insert all records to the `DBTIER_INITIAL_BINLOG_POSITION` table after scaling `ndbmysqld` pods.	2	23.3.1
37143214	All states of DR not displayed when DR triggered via dbtrecover	cnDBTier didn't display all states of georeplication recovery when the georeplication recovery was triggered using the `dbtrecover` script.	3	24.3.0
37288140	DBTier image versions not updated properly in umbrella values.yaml file for 24.2.2 and 24.3.0 DBTier charts	cnDBTier image versions were incorrect in the `custom_values.yaml` file.	3	24.3.0
37352523	Cndb tier 23.4 Helm chart does not pass Helm Strict Linting	Duplicate labels were generated for ndbmysqldsvc. As a result, users were unable to deploy cnDBTier Helm charts.	3	23.4.4
37202609	During DBTier upgrade from 24.2.1 to 24.3.0-rc.2 patching of statefulset.apps/ndbappmysqld is skipped due to kyverno validation failed and later not retried from post-upgrade job	cnDBTier didn't retry `updateStrategy` patch failures during cnDBTier upgrade.	3	24.3.0
37442733	Helm test is failing on 25.1.100-rc.2	Helm test failed due to incorrect version of `openssl` during HTTPS certificate creation.	3	25.1.100

Table 4-12 (Cont.) cnDBTier 24.2.3 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36142511	Heartbeat status returns 502 error code when accessed via CNDB sub-menu GUI and REST API for NRF	cnDBTier heart beat status API returned "`502 Bad Gateway`" response code in the ASM environment.	3	23.4.0
37401291	DBTier User Guide Needs update for BACKUP_SIZE_GROWTH alarm from 23.1.0	The backup size limit after which the `BACKUP_SIZE_GROWTH` alert is triggered was incorrectly mentioned as 5% instead of 20% in the cnDBTier user guide.	4	23.1.0

Table 4-13 cnDBTier 24.2.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37191116	cndbtier install failing for helm version 3.6.x	cnDBTier installation failed as the Helm charts had an error in `mysqld-configmap-data.tpl`.	2	24.2.1
37173763	dbtrecover not marking all down sites as FAILED	The `dbtrecover` script didn't update the status of all failed sites as FAILED.	2	24.3.0
37175416	Missing Alerts for NDBAPPMYSQLD or NDBMYSQLD	cnDBTier user guide didn't state that `HIGH_CPU` alerts are specific to data nodes.	3	23.4.4
37101586	Procedure to update vertical scaling for mgm pod should be documented	cnDBTier user guide didn't provide the procedure to scale the management pods vertically.	3	24.2.0
37199217	Updating HTTPS certificates when existing HTTPS certificates are expired or need an update	cnDBTier user guide didn't provide the procedure to modify HTTPS certificates.	3	24.3.0
37144276	DBTier 24.2.1 Network policies - Incorrect pod selector for ndbmysqld	Incorrect pod selector was observed for `ndbmysqld` pods when network policy was enabled.	4	24.2.1

Table 4-14 cnDBTier 24.2.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36167347	Executing 60K TPS , IN GR mode 6 channel Replication 30K on each site, ndbmysqld pods Restarted and Replication breaks happen "Got error 4009 'Cluster Failure' from NDB Error_code: MY-001296"	Georeplication broke with the MY-001296 error code. To resolve this, alternate MySQL configurations and values are provided for ndbappmysqld and ndbmysqld pods.	2	23.4.0
36569659	Site addition failing on a setup deployed with Prefix	Details about supported topologies for `ndb_restore` were not provided in cnDBTier documentation.	2	24.1.0

Table 4-14 (Cont.) cnDBTier 24.2.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36575575	Replication break observed on 4 site 6 channel setup post user creation	Replication broke on the multichannel cnDBTier setups after user creation when the setups were deployed with pod prefix.	2	24.1.0
36610826	Password change not getting triggered.	The `dbtpasswd` script didn't support NF password change when capital letters were used in username and password sub-strings.	2	24.1.0
36610763	Password change not working for NF	Password changes using the `dbtpasswd` script didn't work as `occneuser` was not used as the main user in the `dbtpasswd` script.	2	24.1.0
36213951	Constant fluctuation in replication channel after password change is performed	When password encryption was enabled, replication channels fluctuated constantly after changing passwords using the `dbtpasswd` script. The `dbtpasswd` script is fixed to support setups where password encryption is enabled.	2	23.4.0
36750208	Replication down is observed for more than 10 mins during CNDB upgrade from 24.1.0 to 24.2.0-rc.3	Replication broke for more than ten minutes during cnDBTier upgrades. To resolve this, connection timeout was set for MySQL connection attempts in the `db-replication-svc` entry point script.	2	23.1.0
36939472	Data pods going into crash back loop off after restarting 2 data pods	Cluster failures were observed when graceful shutdown was performed on NDB nodes simultaneously within the same node group.	2	23.4.6
36843557	cnDBtier 23.3.1 Not able to restore the Database from the DB backup	cnDBtier wasn't able to restore the database from the database backup as `ndbmtd` pods were not reinitialized when there was a change in certain configurations.	2	23.3.1
36895369	cnDBtier Uplift : 23.1 to 23.3.1 - DR issue	cnDBTier didn't have separate TCP configurations for empty slot IDs used by `ndb_restore` commands during georeplication recovery.	2	23.3.1
36615339	cndb ndbmtd-3 pod for site1 and site2 are going into crashloopback after rollback form 24.3.0rc2 to 24.1.1	`ndbmtd` pods went into the `crashloopback` state after a rollback.	2	24.1.0
36482300	Unable to fetch few metrics on a setup deployed with pod prefix	Users were unable to fetch some metrics on setups deployed with pod prefix.	3	24.1.0

Table 4-14 (Cont.) cnDBTier 24.2.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36484876	On a non-GR setup constant errors are coming for DbtierRetrieveBinLogSizeMetrics and DbtierRetrieveReplicationMetrics in cndb monitor service	Errors were observed for the following metrics in the monitor service on cnDBTier setups where georeplication was not enabled: • `DbtierRetrieveBinLogSizeMetrics` • `DbtierRetrieveReplicationMetrics`	3	24.1.0
36486292	BACKUP_TRANSFER_IN_PROGRESS alert retained on setup post remote transfer	The `BACKUP_TRANSFER_IN_PROGRESS` alert was retained on cnDBTier setup even after the remote transfer was successful.	3	24.1.0
36482364	No RemoteTransferStatus displayed while the backup is being transferred from data pod to replication svc	Remote transfer status (RemoteTransferStatus) was not displayed when the backup was transferred from data pod to replication service.	3	24.1.0
36408701	500 Error returned for Replication Health Status when 1 of the replication service goes down in a 4 site GR setup. 24.1.0rc5 build	Replication health status returned the 500 error code, when one of the replication services went down in a three or four-site georeplication setup.	3	24.1.0
36492775	CNCC GUI does not show Service status as down for Backup Manager service when DB connectivity goes down with mysql pods in CNDB 24.1.0rc6	CNC Console GUI did not show service status as DOWN for the backup manager service when the database connectivity with MySQL pods got disconnected.	3	24.1.0
36515531	CNDB- For ndbappmysqld pods PVC health status shows NA even when pvchealth for ndbapp is set as a true	Additional parameters in the infra monitor section of the `custom_values.yaml` file had to be removed as it misled users to update these non-configurable parameters resulting in errors.	3	24.1.0
36522257	CNDB- We are observing that when we disabled pvchealth for ndb pod it shows PVC Health status as down which is misleading.	PVC health status was displayed as DOWN when PVC health was disabled. This status was misleading as the DOWN status indicates that the PVC is unhealthy.	3	24.1.0
36476550	Replication svc stuck in loop waiting for api pods	The `db-replication-svc` pod did not come up if it was restarted due to memory insufficiency while performing a georeplication recovery.	3	23.2.2
36502572	DBTier 23.4.2 dbtrecover script failling for multichannel deployment	The `dbtrecover` script failed to perform fault recovery when the system failed to communication from `ndbappmysqld` pod to remote site LoadBalancer IP address of `ndbmysqld` pods.	3	23.4.2

Table 4-14 (Cont.) cnDBTier 24.2.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36555687	GR state is retained as "COMPLETED" when DR is re-triggered.	When fault recovery was re-triggered using the dbtrecover script, the georeplication state was retained as "COMPLETED".	3	24.1.0
36517463	dbtrecover script continues execution post error "contact customer support to recover."	The `dbtrecover` script displayed "contact customer support to recover." error message, however the script still continued to run. This error was misleading and had to be corrected.	3	24.1.0
36557242	RestFuzz analysis on unexpected HTTP responses	cnDBTier returned incorrect HTTPS responses: • The system displayed the 404 error code instead of 500 when server IDs did not exist. • The system displayed the 503 or 404 error code instead of 500 in a single site setup. • The system displayed the 404 error code when "backup_id" was not found in the backup transfer REST API response.	3	24.1.0
36570453	With MTA disabled config replication svc logs displaying MTA as enabled	The replication service created MTA enabled logs even when MTA was disabled.	3	24.1.0
36567611	DB Tier Switch Over and Stop Replica API not working without "-k" flag.	The "-k" flags had to be removed from the CURL commands in cnDBTier documents as the "-k" flag bypasses SSL certificate verification while making HTTPS requests which is insecure.	3	24.1.0
36618788	CNDBTier SNMP alerts: Remote site name not present in description of two alerts	Remote site name was not present in the descriptions of two cnDBTier SNMP alerts.	3	24.1.0
36644321	RestFuzz scan results flagged 500 Response codes	The following RestFuzz scan results flagged 500 response codes: • REPLICATION_SVC_RESTFUZZ_SCAN • MONITOR_SVC_RESTFUZZ_SCAN • BACKUP_MANAGER_SVC_RESTFUZZ_SCAN • BACKUP_EXECUTOR_SVC_RESTFUZZ_SCAN	3	23.4.4
36378250	Description is empty for health API when backup is not in progress	Description field within the backup manager service APIs was empty.	3	24.1.0
36689742	During stage 2 of conversion misleading errors are observed	Conversion script displayed incorrect error message during stage 2 and stage 3.	3	24.1.0

Table 4-14 (Cont.) cnDBTier 24.2.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36660329	PCF DB 6 Replication - Users and Grants not replicated across sites	The installation guide did not cover the information that users and grants are not replicated to remote sites when multiple replication channels are configured.	3	23.4.3
36729646	Restore Using Remote Transfer Backup procedure is missing in the document	The fault recovery procedure to restore database from backup with `ndb_restore` did not cover the steps to unzip and tar the backup files as per the restore script requirement.	3	23.4.0
36742330	Automatic Backup fails to transfer files to remote host	Debug log options were not available for `apscheduler`, `werkzeug`, and `paramiko.transport.sftp` in the database backup executor service (`db-backup-executor-svc`) when logger mode was set to debug.	3	23.2.1
36745830	cnDbtier user guide procedure to enable https over replication service is not working	cnDBTier documents didn't have the steps to generate PKCS12 certificate for HTTPS connection between `db-replication-svc`.	3	23.2.3
36961805	Cndbtier 22.4.2 db-monitor-svc pod got password security warn log	Password security warning logs were observed in database monitor service.	3	22.4.2
36613148	Avoid using occne-cndbtier pattern suggestion for DBTIER namespace examples due to OCCNE log ingestion filters	cnDBTier documents didn't clarify that the `occne-cndbtier` namespace name used in the documents is a sample namespace name and users have to configure the name according to their environment.	3	23.3.1
36482352	Misleading errors printed in backup manager logs while backup transfer is in progress	Misleading errors were printed in backup manager logs when backup transfer was in progress.	4	24.1.0
36539352	Correct spellings of response in replication svc logs	Spelling errors were observed in replication service logs.	4	24.1.0
36599370	Enhance DBTRecover logs to point to exact cause of failure.	The `dbtrecover` script displayed misleading error messages in the output.	4	24.1.0
36594743	DBTRecover and DBTPassword version doesn't match with CnDB version	The script versions of `dbtrecover` and dbtpasswd scripts didn't match with the cnDBTier version.	4	24.1.0

Table 4-15 cnDBTier 24.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36167347	Executing 60K TPS , IN GR mode 6 channel Replication 30K on each site, ndbmysqld pods Restarted and Replication breaks happen "Got error 4009 'Cluster Failure' from NDB Error_code: MY-001296"	Georeplication broke with the MY-001296 error code. To resolve this, alternate MySQL configurations and values are provided for ndbappmysqld and ndbmysqld pods.	2	23.4.0
36569659	Site addition failing on a setup deployed with Prefix	Details about supported topologies for `ndb_restore` were not provided in cnDBTier documentation.	2	24.1.0
36575575	Replication break observed on 4 site 6 channel setup post user creation	Replication broke on the multichannel cnDBTier setups after user creation when the setups were deployed with pod prefix.	2	24.1.0
36610826	Password change not getting triggered.	The `dbtpasswd` script didn't support NF password change when capital letters were used in username and password sub-strings.	2	24.1.0
36610763	Password change not working for NF	Password changes using the `dbtpasswd` script didn't work as `occneuser` was not used as the main user in the `dbtpasswd` script.	2	24.1.0
35079001	cndbtier deployment fails if affinity is enabled	cnDBTier deployment failed when pod affinity was enabled in the `custom_values.yaml` file without proper configurations. To avoid this scenario, pod affinity is removed from the `custom_values.yaml` file.	2	22.3.3
36213951	Constant fluctuation in replication channel after password change is performed	When password encryption was enabled, replication channels fluctuated constantly after changing passwords using the `dbtpasswd` script. The `dbtpasswd` script is fixed to support setups where password encryption is enabled.	2	23.4.0
36750208	Replication down is observed for more than 10 mins during CNDB upgrade from 24.1.0 to 24.2.0-rc.3	Replication broke for more than ten minutes during cnDBTier upgrades. To resolve this, connection timeout was set for MySQL connection attempts in the `db-replication-svc` entry point script.	2	23.1.0
36482300	Unable to fetch few metrics on a setup deployed with pod prefix	Users were unable to fetch some metrics on setups deployed with pod prefix.	3	24.1.0

Table 4-15 (Cont.) cnDBTier 24.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36484876	On a non-GR setup constant errors are coming for DbtierRetrieveBinLogSizeMetrics and DbtierRetrieveReplicationMetrics in cndb monitor service	Errors were observed for the following metrics in the monitor service on cnDBTier setups where georeplication was not enabled: • DbtierRetrieveBinLogSizeMetrics • DbtierRetrieveReplicationMetrics	3	24.1.0
36486292	BACKUP_TRANSFER_IN_PROGRESS alert retained on setup post remote transfer	The BACKUP_TRANSFER_IN_PROGRESS alert was retained on cnDBTier setup even after the remote transfer was successful.	3	24.1.0
36482364	No RemoteTransferStatus displayed while the backup is being transferred from data pod to replication svc	Remote transfer status (RemoteTransferStatus) was not displayed when the backup was transferred from data pod to replication service.	3	24.1.0
36408701	500 Error returned for Replication Health Status when 1 of the replication service goes down in a 4 site GR setup. 24.1.0rc5 build	Replication health status returned the 500 error code, when one of the replication services went down in a three or four-site georeplication setup.	3	24.1.0
36492775	CNCC GUI does not show Service status as down for Backup Manager service when DB connectivity goes down with mysql pods in CNDB 24.1.0rc6	CNC Console GUI did not show service status as DOWN for the backup manager service when the database connectivity with MySQL pods got disconnected.	3	24.1.0
36515531	CNDB- For ndbappmysqld pods PVC health status shows NA even when pvchealth for ndbapp is set as a true	Additional parameters in the infra monitor section of the custom_values.yaml file had to be removed as it misled users to update these non-configurable parameters resulting in errors.	3	24.1.0
36522257	CNDB- We are observing that when we disabled pvchealth for ndb pod it shows PVC Health status as down which is misleading.	PVC health status was displayed as DOWN when PVC health was disabled. This status was misleading as the DOWN status indicates that the PVC is unhealthy.	3	24.1.0
36476550	Replication svc stuck in loop waiting for api pods	The db-replication-svc pod did not come up if it was restarted due to memory insufficiency while performing a georeplication recovery.	3	23.2.2
36502572	DBTier 23.4.2 dbtrecover script failling for multichannel deployment	The dbtrecover script failed to perform fault recovery when the system failed to communication from ndbappmysqld pod to remote site LoadBalancer IP address of ndbmysqld pods.	3	23.4.2

Table 4-15 (Cont.) cnDBTier 24.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36555687	GR state is retained as "COMPLETED" when DR is re-triggered.	When fault recovery was re-triggered using the dbtrecover script, the georeplication state was retained as "COMPLETED".	3	24.1.0
36517463	dbtrecover script continues execution post error "contact customer support to recover."	The `dbtrecover` script displayed "contact customer support to recover." error message, however the script still continued to run. This error was misleading and had to be corrected.	3	24.1.0
36557242	RestFuzz analysis on unexpected HTTP responses	cnDBTier returned incorrect HTTPS responses: • The system displayed the 404 error code instead of 500 when server IDs did not exist. • The system displayed the 503 or 404 error code instead of 500 in a single site setup. • The system displayed the 404 error code when "backup_id" was not found in the backup transfer REST API response.	3	24.1.0
36570453	With MTA disabled config replication svc logs displaying MTA as enabled	The replication service created MTA enabled logs even when MTA was disabled.	3	24.1.0
36567611	DB Tier Switch Over and Stop Replica API not working without "-k" flag.	The "-k" flags had to be removed from the CURL commands in cnDBTier documents as the "-k" flag bypasses SSL certificate verification while making HTTPS requests which is insecure.	3	24.1.0
36618788	CNDBTier SNMP alerts: Remote site name not present in description of two alerts	Remote site name was not present in the descriptions of two cnDBTier SNMP alerts.	3	24.1.0
36644321	RestFuzz scan results flagged 500 Response codes	The following RestFuzz scan results flagged 500 response codes: • REPLICATION_SVC_RESTFUZZ_SCAN • MONITOR_SVC_RESTFUZZ_SCAN • BACKUP_MANAGER_SVC_RESTFUZZ_SCAN • BACKUP_EXECUTOR_SVC_RESTFUZZ_SCAN	3	23.4.4
36378250	Description is empty for health API when backup is not in progress	Description field within the backup manager service APIs was empty.	3	24.1.0
36689742	During stage 2 of conversion misleading errors are observed	Conversion script displayed incorrect error message during stage 2 and stage 3.	3	24.1.0

Table 4-15 (Cont.) cnDBTier 24.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36660329	PCF DB 6 Replication - Users and Grants not replicated across sites	The installation guide did not cover the information that users and grants are not replicated to remote sites when multiple replication channels are configured.	3	23.4.3
36729646	Restore Using Remote Transfer Backup procedure is missing in the document	The fault recovery procedure to restore database from backup with `ndb_restore` did not cover the steps to unzip and tar the backup files as per the restore script requirement.	3	23.4.0
36742330	Automatic Backup fails to transfer files to remote host	Debug log options were not available for `apscheduler`, `werkzeug`, and `paramiko.transport.sftp` in the database backup executor service (`db-backup-executor-svc`) when logger mode was set to debug.	3	23.2.1
36482352	Misleading errors printed in backup manager logs while backup transfer is in progress	Misleading errors were printed in backup manager logs when backup transfer was in progress.	4	24.1.0
36539352	Correct spellings of response in replication svc logs	Spelling errors were observed in replication service logs.	4	24.1.0
36599370	Enhance DBTRecover logs to point to exact cause of failure.	The `dbtrecover` script displayed misleading error messages in the output.	4	24.1.0
36594743	DBTRecover and DBTPassword version doesn't match with CnDB version	The script versions of `dbtrecover` and dbtpasswd scripts didn't match with the cnDBTier version.	4	24.1.0

Note:

Resolved bugs from 23.3.3, 24.1.1, and 23.4.6 have been forward ported to Release 24.2.1.

4.2.4 CNE Resolved Bugs

Table 4-16 CNE 24.2.6 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36874451	CNE `lb-controller` pods stops processing service events or producing logs	The `lb-controller` pod stalled and did not function and displayed the following exception in the logs. This exception was seen intermittently. `FileNotFoundError: [Errno 2] No such file or directory: '/etc/exabgp/log'`	3	24.2.6
37842711	CNE installation failure	In the latest OL9 release, partitions were created differently, and the CNE `cloud_growpart` tasks required specific configuration. This resulted in bastions that lacked enough space to handle all their dependencies and configuration file.	4	25.1.100

Table 4-17 CNE 24.2.4 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37033023	Replacing a Controller node for CNE (CNLB based, version 24.2.0) giving error	The system ran into an error when a controller node was replaced in a CNLB based CNE.	2	24.2.0
37363771	CNLB ips not accessible in thrust3 cluster	CNLB IPs were not accessible causing the CNLB pods to restart frequently.	2	24.3.0

Table 4-17 (Cont.) CNE 24.2.4 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37021718	After upgrade to 23.4.6 OCCNE still we are facing same issue reported in 23.4.4 lbvm pair is not taking traffic	The IP rule was missed during switchovers causing the traffic management to fail.	2	23.4.6
37398635	cnlb pods restarting on thrust3(24.3.0)	CNLB IPs were not accessible causing the CNLB pods to restart frequently.	3	24.3.0
37040679	vCNE opnstack upgrade failure with Local DNS enabled due to missing auto plugin config	When Local DNS was enabled, vCNE OpenStack upgrade failed due to a missing auto plugin configuration.	3	24.1.1

Table 4-18 CNE 24.2.3 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37233610	OCCNE User guide 6.3.8 Performing an etcd Data Backup not working	While running the `etcd_backup.sh` script, `occne-etcd-backup` PVC failed to bind. It was observed that the PVCs with the "`standard`" storage class had `readWriteOnce` access mode, whereas `etcd-backup` got created with `ReadWriteMany` access mode.	3	22.4.3
37239612	VMware missing egress NAT rules on LBVM	`lb-controller` didn't install the Source Network Address Translation (SNAT) rules for egress communication. During the `lb-controller` restart and switchover, the expected `MASQUERADE` rule didn't show up on the new active Load Balancer.	3	24.2.1

Table 4-19 CNE 24.2.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37161841	OCCNE 23.4.1 (LBVM patch 23.4.6) : Security groups are removed from the ports during switchover.	When the compute node hosting the ACTIVE LBVM (OAM01) was shut down, the system performed a switchover to OAM02. However, the security groups were removed from the ports and got attached to the new active LBVM (OAM02).	2	23.4.1
37027492	lbvm switchover not happening due to errors in lb-controller pod	`lb-controller` failed to perform a LBVM switchover when the OpenStack compute node hosting ACTIVE LBVM was shut down.	3	23.4.1

Table 4-20 CNE 24.2.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36958805	bastion failover not working with slow network speed to central repo	The Bastion HA switchover failed due to slow image transfer from CENTRAL_REPO host.	2	23.4.4
36764539	Different private interface names to cause failure	The private internal interface name for all servers (bastion/node/lbvm/master) was ens192. From release 23.3.x, the private internal interface names were changed from ens 192 to ens160 after the OS installation on VMware clusters. The value of private_lbvm_interface is hardcoded from ens192 to ens160. In CNE 24.1.x and OL9.4, there was a private_lbvm_interface failure as the internal interface name was ens192 instead of ens160.	3	24.1.0

Table 4-20 (Cont.) CNE 24.2.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36877689	lb-controller fails to install egress NAT rules on LBVM	The private internal interface names for all servers (bastion/node/lbvm/master) were ens192. From release 23.3.x, the private internal interface names were changed from ens 192 to ens160 after the OS installation on VMware clusters. The value of private_lbvm_interface is hardcoded from ens192 to ens160. With CNE 24.1.x and OL9.4, there was a private_lbvm_interface failure as the internal interface name was ens192 instead of ens160.	3	24.1.0
36975460	exabgp.conf file not getting configured in occne-lb-controller pod	The `exabgp.conf` file does not include the neighbor list. The code in the lb controller, which created a child process to configure the `exabgp.conf` file, failed but the parent was not aware of this failure. The parent continued to run and the lb controller pod came up with the incomplete neighbor list in the `exabgp.conf` file.	3	24.1.0
36893817	Intermittent connectivity issue to LoadBalancer service	After deploying the CNE cluster, the `cluster_test` failed as the service IPs from the Bastion host were unreachable. The ARP entry for gateway (ToR switches' VRRPv3 VIP) was missing while running the tcpdump.	3	23.4.4

Table 4-20 (Cont.) CNE 24.2.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36937440	Opensearch master nodes PVC getting full	Opensearch master nodes were getting created with the role of "master,data". This caused master nodes to act as data nodes. OCCNE configuration offered master node only for cluster management because of which node.roles value must be changed to "master" from "master,data".	3	23.4.4
37094904	rook-ceph-OSD Total pod's are not coming up post worker node reboot	When nodes were rebooted, it was not guaranteed that Linux devices (during discovery) will be assigned with the same id. This caused rook-ceph pods failed to come up. This was a bug in rook ceph. rook version uplift fixed the bug.	3	24.2.0
37121745	lb-controller database has inconsistency with the deployed LoadBalancer services	When `ingress_network_daemon.service` failed, it caused inconsistency in the lb-controller database with the deployed LoadBalancer services.	3	24.1.0

Table 4-21 CNE 24.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36573356	After Upgrade from 23.4.0 to 24.1.0-rc.6, Metrics for cluster disk usage shows no data.	After an upgrade from 23.4.0 to 24.1.0, the metrics for cluster disk usage did not display any data.	3	24.1.0
36596625	AddworkerBM.py failing at OS prov due to not updating the /etc/hosts	Adding worker nodes using the script failed during the OS provisioning stage as the `/etc/hosts` file was not updated with the worker node entry.	3	23.4.1

Table 4-21 (Cont.) CNE 24.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36316652	Bastion DNS forwarders failing to resolve openstack auth to worker nodes (DNSsec issue)	Improper name servers amendment in worker nodes, Bastion, and control nodes caused the deployment to fail while trying to access control nodes.	3	23.4.0
36319935	DNS Server Failure sent from bastion to worker nodes	During a DNS query, external server responded to the DNS query, however issues were observed when the Bastion transferred the response to Kubernetes worker nodes.	3	23.4.0
36567050	addBMWorker.py Task restart ceph pod fails incorrectly due to name convention and check	Adding a worker node using the `addBmWorkerNode.py` script failed due to incorrect naming convention and check conditions (pods_count == nodes_count).	3	23.4.1
36569672	Not clearing "DEPLOY IN PROGRESS" banner after addition of Worker node	While adding a worker node, the `DEPLOY IN PROGRESS` banner did not clear even after the worker node was added.	3	23.4.1
36196178	Add Kubernetes Worker Node using addBmWorkerNode.py failed	Adding a worker node using the `addBmWorkerNode` script failed with the following error: "Unable to instantiate AddBmWorkerNode class.."	3	23.2.5
36299104	Failures trying to recreate LBVM using documented DR steps	While recovering a failed Load Balancer VM (LBVM), the recovery ran into issues due to low disk space. LBVM log rotation is configured to avoid filling the disk space which caused the LBVM to crash.	3	22.4.5

> **Note:**
>
> Resolved bugs from 24.1.x have been forward ported to Release 24.2.0.

OSO 24.2.5 Resolved Bugs

There are no resolved bugs in this release.

OSO 24.2.0 Resolved Bugs

There are no resolved bugs in this release.

4.2.5 NEF Resolved Bugs

Table 4-22 NEF 24.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36751895	During in solution upgrade of NEF in a 2 site GR setup, while upgrading CNCC from 24.1.0 to 24.2.0 rc2, CNDB replication is broken	During in-service solution upgrade of NEF in a 2 site GR setup, while upgrading Cloud Native Core Console from 24.1.0 to 24.2.0, a broken replication was observed.	2	24.2.0
36611047	NEF-CNCC: - Some of the parameters are not updated in CNCC after Doing helm upgrade.	Some of the parameters and GMLC value were not getting updated in CNC Console after performing Helm upgrade.	2	24.1.0
36635995	NEF-CNCC: - Monitoring Events - "Destination If LocQOS Absent" and "Switch to UDM failure" functionality not working	The Monitoring Events functionalities of Destination If LocQOS Absent and Switch to UDM failure were not working.	2	24.1.0
36578399	msisdnless-mo-sms : OFR callflow is by passing ext-nef-egress-gw from mo-sms service to AF.	OFR callflow was bypassing `ext-nef-egress-gw from msisdnless-mo-sms` service to AF.	2	24.1.0
36551727	Although the "switchToPCRFOnAuthFailure" enabled , the subscription request is not hitting the PCRF	Even though the `switchToPCRFOnAuthFailure` parameter was enabled, it was observed that the subscription request was not reaching the PCRF.	2	24.1.0

Table 4-22 (Cont.) NEF 24.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36798043	Unable to update the request timeout of QOS jetty client , which is causing the call flow to fail	The request timeout was different in deployment and CNC Console was causing the subscription to fail. Hence, the request timeout of QoS jetty client could not be updated.	2	24.2.0
36744717	NEF-CNCC: - When GMLC is disabled edit ICON should be disabled as its read only parameter	When GMLC was disabled, the edit icon should also have been disabled as it is a read-only parameter. It was observed that the icon was not displayed as disabled.	3	24.2.0
36656809	NEF-CNCC: - QOS Configuration - Eventhough QOS subscription is failed still call exist in the DB	While performing QoS configuration, call still existed in the database even when the subscription failed.	3	24.1.0
36647686	NEF-CNCC: - QOS Configuration - "Switch To PCRF On PCF Authorization Failure" Feature - Only 404 error code and Error Response TBC mentioned in the user guide and Requirement page	For QoS configuration, in Switch To PCRF On PCF Authorization Failure feature, only 404 error code is provided in User Guide and Requirements page. Information about other error responses were also needed to be updated.	3	24.1.0
36647362	NEF-CNCC: - QOS Configuration - Help Icon is not working for the QOS configuration Tab	For QoS configuration, the Help icon in the QoS configuration tab was not showing any information about QoS.	3	24.1.0

Table 4-22 (Cont.) NEF 24.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36580287	msisdnless-mo-sms : invalid IMSI and MSISDN format allowing and same sending towards UDM	NEF was allowing `msisdnless-mo-sms` services with IMSI and MSISDN, which were not invalid. The same was then sent towards UDM.	3	24.1.0
36584726	msisdnless-mo-sms : Supported Features always sending zero towards AF	When an OFR request was sent from SMS-SC to NEF with Supported Features AVP, the Supported Features were always sending back "0" towards AF.	3	24.1.0
36610071	NEF-CNCC: - Incorrect Feature status updated in the "System configuration"	Incorrect feature status was getting updated in the system configuration about MSISDNless MO SMS.	3	24.1.0
36610261	NEF-CNCC: - "NEF" information is displayed in "CNDBTier" Tab	NEF information was displayed in cnDBTier tab, even when there was no cnDBTier added.	3	24.1.0
36610551	NEF-CNCC: - Monitoring Events - "switchOnErrorCodes" contains two parameters but in CNCC its displaying as one parameter "CodeCause"	In Monitoring Events, switchOnErrorCodes consisted of two parameters but in CNC Console, it was displaying as one parameter CodeCause.	3	24.1.0
36635736	NEF-CNCC: - Monitoring Events - Even though "Location type"(mandatory parameter) is absent Montioring subscription is getting success.	In Monitoring Events, even though `Locationtype` (mandatory parameter) is absent, the Monitoring subscription was getting success status.	3	24.1.0

Table 4-22 (Cont.) NEF 24.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36641482	NEF-CNCC: - Monitoring Events - Explicit Cancellation functionality not working for both Maximum Reports and GMLC initiated Notification	In Monitoring Events, the explicit cancellation functionality was not working for both maximum reports and GMLC initiated notification.	3	24.1.0
36580033	msisdnless-mo-sms : NEF is not rejected with external id which is not in correct format	NEF did not reject the `msisdnless-mo-sms` request even when the external id was not in the correct format.	3	24.1.0
36578766	msisdnless-mo-sms : metrics :- ocnef_msisdnless_mo_sms_srv_latency metric "time" Dimension missing in the output	When sending OFR request from SMS-SC to NEF in `ocnef_msisdnless_mo_sms_srv_latency` metric. the `time` parameter was missing in the output.	3	24.1.0
36577899	msisdnless-mo-sms : IMS support for the for OFR message	More information was needed to be added in the NEF User Guide about IMS support for the OFR message.	3	24.1.0
36574636	msisdnless-mo-sms : Auth-seesion state avp coming two times in OFA response	When OFR request was sent from SMS-SC to NEF with Auth-Session-State values, state avp was sent two times in OFR response.	3	24.1.0

Table 4-22 (Cont.) NEF 24.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36570391	QOS update Procedure : when the notification destination parameter was configured to null the response code of 200 was observed and the parameter "notification-destination" was deleted in the DB	While performing QoS update, when the `notification-destination` parameter was set to Null, 200 response code was received. It was identified that the `notification-destination` parameter was deleted in the database.	3	24.1.0
36567991	msisdnless-mo-sms : OFR with Auth-Session-State other than 0 and 1 values NEF is not rejected.	NEF was not rejecting OFR msisdnless-mo-sms requests sent with Auth-Session-State other than 0 and 1 values.	3	24.1.0
36567875	msisdnless-mo-sms : OFR with Auth-Application-Id and Acct-Application-Id parameters NEF is sending success code.	NEF was sending success code for OFR `msisdnless-mo-sms` requests with `Auth-Application-Id and Acct-Application-Id` parameters.	3	24.1.0
36567508	msisdnless-mo-sms : Vendor-Specific-Application-Id without Auth-Application-Id and Acct-Application-Id OFR message not rejected	NEF was not rejecting OFR msisdnless-mo-sms messages with Vendor-Specific-Application-Id without Auth-Application-Id and Acct-Application-Id.	3	24.1.0
36567023	msisdnless-mo-sms : DRMP((Diameter Routing Message Priority) value is Allowing all the enum values	NEF was accepting all DRMP ENUM values in msisdnless-mo-sms, even the ones not defined in specification.	3	24.1.0

Table 4-22 (Cont.) NEF 24.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36562177	msisdnless-mo-sms : AF response code should be "200" instead of "204" in AF response stubs.	The 204 result code was sent instead of 200 from AF stub towards NEF.	3	24.1.0
36499347	ME update call flow description response code should be 200.	The response code mentioned in NEF User Guide for ME update call flow was required to be updated to 200.	3	24.1.0
36347401	Invalid monitor expire time accepted during ME update procedure for some dates.	While performing ME update, it was observed that, for some dates, invalid monitor expire time was getting accepted.	3	23.4.0
36337334	GATEWAY_TIMEOUT error code 504 should be updated in the User guide for ME subscription.	The `GATEWAY_TIMEOUT` error code 504 was required to be updated in the NEF User Guide for ME subscription.	3	23.4.0
36317632	Error code and Error cause should be correct for the ME "locationType": "LAST_KNOWN_LOCATION" for PUT and POST Operation.	For PUT and POST operations, error code and error cause had wrong values for ME "locationType": "LAST_KNOWN_LOCATION".	3	23.4.0
36300631	"eventTime" not sending towards AF During ME Location Reporting Notification.	For ME subscription, `eventTime` parameter was missed in the notification information sent towards AF.	3	23.4.0
36295767	invocationTimeStamp in the Charging Data Request should be in date-time format	The `invocationTimeStamp` in the Charging Data request was required to changed to date-time format.	3	23.4.0

Table 4-22 (Cont.) NEF 24.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36295686	aPITargetNetworkFunction of nEFChargingInformation in the Charging Data Request should contain mandatory parameter "nodeFunctionality"	The `nodeFunctionality` parameter was missing in aPITargetNetworkFunction of nEFChargingInformation in the Charging Data request.	3	23.4.0
36293429	During ME pdu session notification - GPSI parameter accepting without extid - and msisdn -	While performing ME PDU session notification, `GPSI` parameter was getting accepted even without extid and msisdn.	3	23.4.0
36276299	During ME update procedure NEF sending same subscriptionId towards UDM for all ME update subscription.	While performing ME update, NEF was sending same `subscriptionId` towards UDM for the ME update subscription.	3	23.4.0
36203683	TI subscription with PCF(IPV6) Is throwing error as "Connection refused to 5gc core"	When TI subscription with IPV6 stored in PCF was sent, `Connection refused to 5gc core` error was received.	3	23.4.0
35897663	Capif :-23.3.0: Discovery-group : Delete Discover group is not deleting some of the Discovery-group created	The DELETE command to delete Discover Group was not deleting some of the created Discovery groups.	3	23.3.0
35609204	NEF-TLS Enable :23.2.0 :GR : 2.1ktps traffic on both sites :During long run (63hr) ndbmtd-1 and ndbmysqld-1 pod restarted one time at site2-cndb2.	While performing long run for 63 hours, it was observed that ndbmtd-1 and ndbmysqld-1 pods restarted once at site2-cndb2.	3	23.2.0

Table 4-22 (Cont.) NEF 24.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35429399	Model -B : TI subscription: gNbId object with bitLength parameter is not available in geoZoneIdToSpatialValidityMap configuration.	When TI subscription request was sent, gNbId object with bitLength parameter was not available in `geoZoneIdToSpatialValidityMap` configuration.	3	23.1.0
35387259	TI subscription with externalgroup id rejecting with subscriber already exist for some external group id.	When TI subscription request was sent with externalgroup ID, some external group IDs were rejected stating as "Subscriber Already Exist".	3	23.1.0
35308131	TI Update subscription allowing ethtraffic filters to update UE- ipv4/v6 session	When updating TI subscription, it was observed that the ethtraffic filters were allowing to update UE- ipv4/v6 session.	3	23.1.0
35065670	Some of the external id's are throwing error for the "already subscription exist" even though subscription is not exist in cnDB	It was observed that some of the external IDs were throwing Subscriber Already Exist" error even for the subscription that did not exist in cnDB.	3	22.4.0
36776204	Data-type for GPSI is mentioned wrong in the NEF REST API SPECIFICATION GUIDE	Datatype for GPSI was needed to be updated added in the NEF REST API Guide.	3	24.2.0
36776192	NEF: ME Notification - Even though the GPSI format is incorrect, the notification is being validated.	NEF was validating a invalid GPSI format.	3	24.2.0

Table 4-22 (Cont.) NEF 24.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36772843	Model-D-msisdnless-mo-sms : OFR (OFR-SGd-Request (OFR-SGdR)) notification is success when AF sends 404 error code.	NEF was sending 2001 success code instead of 404 error code, when OFR-SGd-Request notification was sent towards diametergateway.	3	24.2.0
36538782	msisdnless-mo-sms alerts :-"#unique_195" - some links are missing in msisdnless-mo-sms service alerts	Broken hyperlinks were identified in NEF User Guide in `MSISDNLessMoSMSShortCodeConfigMatchFailure` alert section.	4	24.1.0
36506009	Grafana Metric json Title should be Generic ("OCNEF-Metric") not service specific("OCNEF-Metric-Jazz-Msisdnlessmosms-1")	Grafana Metric JSON title was required to be updated to Generic ("OCNEF-Metric") from service specific ("OCNEF-Metric-Jazz-Msisdnlessmosms-1").	4	24.1.0
36477521	NEF ATS 24.1.0.rc-2 - CNCC ATS TC failing in Jenkins GUI when run in one go	While running CNC Console ATS in Jenkins GUI, testcase was failing.	4	24.1.0

Note:

Resolved bugs from 23.4.x have been forward ported to Release 24.2.0.

4.2.6 NRF Resolved Bugs

Release 24.2.4

Table 4-23 NRF 24.2.4 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37826816	Secondary NRF sending 500 internal server error towards SMSF when primary NRF is taken out of service	There were instances where an NF registered at NRF without the ‘nfFqdn’ attribute was required to move to another NRF due to maintenance activity or other reasons. In such cases, if the NF sent an NfRegister/NfUpdate/NfDeregister request to the other NRF during the switchover, the request failed with a 500 error response. This was occurring due to an exception encountered while pegging the metric `ocnrf_nf_switch_over_total` metric, which required the nfFqdn and the profile does not contains the nfFqdn. The issue was occurring only for those profiles registered without the nfFqdn, and during switch over it sends NfRegister/NfUpdate/NfDeregister. (NfHeartbeat was working as expected.)	1	24.2.3
37432510	Subscription pod stuck in congested state due to pending message count	Subscription pod got stuck in overload state due to pending message count. The pending message count did not decrease even after all traffic was halted, which kept the subscription pod in an overflow condition indefinitely.	2	23.4.6
37584637	NRF not considering local Subscriptions from local db dip upon 100% packet loss with Cache pods - Growth feature enabled	NRF was not considering the local subscriptions from local db dip upon 100% packet loss with NRF Cache Data Service Microservice pods -(Growth feature enabled). NRF stopped sending the NFStatusNotify service operations and local subscriptions are not considered for generating the NFStatusNotify service operation messages.	2	24.2.4

Table 4-23   (Cont.) NRF 24.2.4 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37643446	Upgrade Failed DB replication	Replication was getting broken due to absence of the records on the another site. During this it is found that the backup tables of nrfNetworkDB database (NfScreening_backup, NrfSystemOptions_backup, SiteIdToNrfInstanceIdMapping_backup) did not have primary key columns. NfScreening_backup, NrfSystemOptions_backup have JSON Column (BLOB) and MYSQL does not support replication in such cases.	2	23.4.6
37722198	NRF 23.4.6 upgrade is ignoring tai/tac in discovery request	NRF 23.4.6 upgrade ignored tai/tac in discovery request. During NF profile processing, if a profile does not match the query parameter, the smfInfoList is set to null and updated in the original profile. As a result, when forwarding, NRF returned an empty response. In this case, NRF treated all profiles as eligible, as profiles without an *smfInfoList* can be selected for any S-NSSAI, DNN, TAI, and access type.	2	23.4.6
37433162	NRF is stuck in L4 Overload state due to continuous Reset stream received for more than 1-hour from perfgo(consumer NF)	NRF is stuck at L4 Overload state due to continuous Reset stream received for more than 1-hour. The pending count was high at Ingress gateway due to number of channels open towards back end. It was observed that Ingress gateway considered the requests as time out even before the request timeout had occurred.	2	23.4.6
37415555	NRF is stuck in L4 Overload state though all ingress pods are back to functional and Running after planned multiple(7 to 12/27) ingress pods restart continuously for 15 min.	NRF was stuck at L4 Overload state due to continuous restart of Ingress Gateway pods. The pending count was high at Ingress gateway due to number of channels open towards back end. It was observed that Ingress gateway considered the requests as time out even before the request timeout had occurred.	2	23.4.6

Table 4-23 (Cont.) NRF 24.2.4 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37629783	ATS: new feature test cases Config39_SlfReroutesCheck.feature failing	The new feature test cases Config39_SlfReroutesCheck.feature failed as there was a mismatch in the response due to the hardcoded value in oncrfPort. The hardcoded value is now changed to a variable such that it can take values from the system.	3	24.2.2
37633507	ocnrf.forward.nfDiscover.rx.responses is not pegged for alternate NRF retry	The *ocnrf_forward_nfDiscover_rx_responses* metric was not pegged while trying for an alternate NRF. However, the *ocnrf_forward_nfDiscover_tx_requests* metric was getting pegged twice while trying for an alternate NRF.	3	24.2.0
37696286	Sending of Accept-Encoding header with value as GZIP under configurable flag	Accept-Encoding header sent with value as **gzip** without any configurable option. This resulted in non-backward compatible.	3	24.2.2
37633397	ocnrf_nfDiscover_profiles_discovered_total metric is not pegged in forwarding scenarios	During a forwarding discovery request, the metric *ocnrf_nfDiscover_profiles_discovered_total* was not pegged in the call flow and processing. Instead, the *ocnrf_nfDiscover_profiles_discovered_total* metric was getting pegged.	3	23.4.6
37760760	allow-ingress-sbi should have ports for https connections	Incorrect Ingress Gateway port number was added in NRF network policy's allow-ingress-sbi section for https connections. Due to this, applying NRF network policies was not working as expected because https request towards Ingress Gateway was not allowed due to incorrect port being allowed.	3	24.2.4
37637752	After restarting EGW pods multiple times, Prometheus is not showing EGW outgoing connections	When Egress Gateway pod was restarted multiple times, Prometheus was not showing values properly for Egress Gateway outgoing connections.	4	24.2.4

Release 24.2.3

NRF 24.2.3 is a Critical Patch Update. Critical Patch Updates provide security patches for supported Oracle on-premises products. They are available to customers with valid support contracts.

For more information, see Critical Patch Updates, Security Alerts, and Bulletins.

Table 4-24   NRF 24.2.3 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37481951	NRF upgrade failed with cause "post-upgrade hooks failed"	NRF upgrade failed with cause "post-upgrade hooks failed".	2	23.4.6
37481908	NRF - Multiple 5xx,4xx Error observed during one of the two app-info pod restart continuously for 15 min.	Multiple 5xx, 4xx errors were observed in NRF when one of the two app-info pods restarted continuously for 15 minutes.	3	23.4.6
37481924	NRF is rejecting NFSetId attribute with uppercase value in Registration Request payload	NRF rejected the NFRegister service operation with invalid NF Set Id (For example, UDR Registration with upper NFType - UDRSet). Prior to 23.4.0, NRF allowed both upper and lower case NF Set IDs. However, from 23.4.0, NRF rejected the NFRegister with NF Set ID in upper case. This rejection is valid if the format is not as per 3GPP, but the behavior should be controlled by a flag to minimize network impact during upgrade. With this fix, an option is provided to enable the 3GPP based behavior, when all of the NFs gets compliant to 3GPP defined NF Set ID format.	3	23.4.0
37000019	Subset Of SCP Peers Unhealthy After OPTIONS Not Sent By NRF EGW	Subset of SCP peers was unhealthy after OPTIONS were not sent by NRF Egress Gateway Service.	3	23.4.1

NRF ATS 24.2.3 Resolved Bugs

Table 4-25   NRF ATS 24.2.3 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37485652	ATS cases are failing Invalid fqdn variable in the registration JSON	ATS cases failed when an invalid FQDN was sent in the registration JSON. This caused timeout in Egress Gateway microservice.	3	23.4.0

Release 24.2.2

Table 4-26   NRF 24.2.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37100137	NRF uses the wrong error code when incoming gzip encoded content is received	NRF sent 400 response code when incoming request was gzip encoded instead of 415.	2	24.1.0

Table 4-26 (Cont.) NRF 24.2.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37188601	NRF sending "additionalAttributes" in NF subscription response is causing issues in AUSF/UDM	NRF was sending "additionalAttributes" in NFStatusSubscribe service operation response.	2	23.4.4
37111123	NRF includes accept-encoding header with value gzip in responses even though NRF doesn't support incoming gzip encoding content	NRF included the `accept-encoding` header with value gzip in responses even though NRF was not supporting incoming gzip encoding content.	3	24.1.1
37203105	NRF DBTier custom values yaml file updates as per recommendations for ndb parameters and vertical pvc scaling	NRF cnDBTier custom values yaml file was updated as per recommendations for ndb parameters and vertical pvc scaling.	3	24.2.1
37152447	NRF 24.2.2:W2 NRF-Alarm for inactive DbReplicationStatus	NRF was sending alarm for inactive `DbReplicationStatus` in NRF auditor microservice.	3	23.4.4

NRF ATS 24.2.2 Resolved Bugs

Table 4-27 NRF ATS 24.2.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37203082	NRF ATS test cases failing due to Timeout exception in egress gateway for unknown host	NRF ATS test cases failed due to timeout exception in egress gateway for unknown host.	3	24.1.3
37203053	ATS : slfCandidateList is not populated	`slfCandidateList` in ATS is not populated.	3	24.1.3

Release 24.2.1

Table 4-28 NRF 24.2.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
36945520	NRF Discovery requests failure after NRF upgrade to 23.4.2.	When a discovery query was sent to CDS (new microservice in 23.4.x) and CDS queried the database to fetch the profiles, if the database query failed due to exception, discovery query flushed out all the profiles from its in-memory cache.	1	23.4.2
37050747	Upgrade from 24.1.0 to 24.2.0 failed	In the Openshift environment, the `runc` command was unable to access the jars and the entry point files, which caused NRF upgrade failure.	3	24.2.0

NRF ATS 24.2.1 Resolved Bugs

Table 4-29 NRF ATS 24.2.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37070481	NRF ATS 24.1.2 - Random regression test case failures	While doing full regression testing, random features failed while verifying the responses received from `slfOptions`.	3	24.1.2

Release 24.2.0

Table 4-30 NRF 24.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
36698413	requester-snssais field misspelled in URL encoding during fowarding/ roaming	The `requester-snssais` discovery query attribute was misspelled in URL encoding during forwarding/roaming scenarios.	3	24.1.1
36695260	After NRF upgrade to 23.4.2 aud claim in oauth token is causing 401 UNAUTHORIZED failures	After NRF upgrade to 23.4.2 `aud claim` in oAuth token was causing 401 UNAUTHORIZED failures. This failure occurred as third party library changed its behaviour by sending `aud` attribute in AccessTokenClaims as arrayed for NFType value instead of a string type value	3	23.4.2
36610232	Incorrect Error code ONRF-SUB-SUBSCR-E0100 for cause MANDATORY_IE_MISSING	NRF sent an incorrect error code as *ONRF-SUB-SUBSCR-E0100* when MANDATORY_IE_MISSING was for NFStatusSubscribe Service operation in the error response message.	3	24.1.0
36561208	Incorrect Error code ONRF-ACC-ACROAM-E0399 for scenario NRF peer 5xx response received	NRF was mapped to an incorrect E0399 error code instead of E0301 for the For 5xx response from the peer in the AccessToken roaming flow. NRF now maps 5xx response from peer in AccessToken roaming flow to E0301 error code.	3	24.1.0
36542350	OcnrfReplicationStatusMonitoringInactive alert is incorrectly getting raised.	Metric `ocnrf-replication-status-check` was not getting pegged when the flag `overrideReplicationCheck` flag was set to true. This raised a false alert.	3	24.1.0

Table 4-30 (Cont.) NRF 24.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
36509805	Cause attributes of 3GPP services need to be corrected for some of the instances	The error returned when a discovery request was sent with search data that had an incorrect optional query parameter was returning errors with the cause **MANDATORY_QUERY_PARAM_INCORRECT** instead of the correct error cause **OPTIONAL_QUERY_PARAM_INCORRECT**.	3	23.4.0
36507713	Unable to remove peer, peer-set and route configuration in EGW via NRF CNC Console GUI	Egress Gateway configurations for peer, peerset, and routesconfiguration did not support DELETE API calls.	3	24.1.0
36501153	"errorHandling" field missing in NRF CNC Console GUI EGW Routes Configuration	ErrorHandling field was missing from NRF CNC Console GUI as an incorrect JSON model was used.	3	24.1.0
36499847	Unable to remove error code from error code profiles and error code series "id" from Error Code Series via CNCC	Error code profiles and error code series could not be deleted using the CNC console as DELETE API calls were not supported in Ingress Gateway configurations.	3	24.1.0
36409410	NRF network policies for SBI ingress-gateway	Incorrect Ingress Gateway port number was added in NRF network policy's **allow-ingress-sbi** section for https connections.	3	23.4.0
36159212	ocnrf_nfInstance_status_change does not peg nfFqdn dimension when if XFCC header is not present.	The value of the nfFqdn dimension was not retrieved from the nfProfiles for the metric **ocnrf_nfInstance_status_change** and instead the UNKNOWN value was pegged.	3	23.4.0
35937121	UAH propagation is happening for SLF queries	NRF propagated the User-Agent Header received in the discovery request via SCP/curl command for SLF queries.	3	23.3.0
35865509	NRF Upgrade to 23.1.3 Caused the replication switchover	NRF upgrade to 23.1.3 caused the replication switchover.	3	23.1.3
35656001	NRF- subject in jwt token getting failed when sent with upper case in CCA header for feature - CCA Header Validation	CCA header validation failed as Ingress Gateway did not add a case-insensitive check for the *sub* field.	3	23.2.0
35464979	Change in number of NF Notification Retries observed for Feature - Notification Retry	There were changes in the number of NF Notification Retries observed for the Notification Retry feature.	3	23.1.0

Table 4-30 (Cont.) NRF 24.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
34611851	NRF-discovery sending incorrect response with EmptyList nf profiles when nfServiceStatus is SUSPENDED	During the processing of `NFDiscover` service operation, when emptyList feature was enabled, NRF was not sending NFProfiles, where both NFProfileStaus and NFServiceStatus were SUSPENDED.	3	22.4.0
34205871	3gpp-Sbi-Correlation-Info header not populated in response generated from IGW	The 3gpp-Sbi-Correlation-Info header present in the request was not getting copied to the failure responses generated from Ingress Gateway.	3	22.2.0
34205684	OCNRF Preferred locality in NFDiscovery query attributes values having plus symbol or space is generating null pointer in NRF Forwarding use-cases	The Preferred-Locality in NFDiscovery query attributes were generating a null pointer in NRF Forwarding use-cases when the value had a plus sign or a space in it. This issue occurred as decoding of NFDiscover Service operation query at first NRF and encoding of NFDiscover Service operation query while forwarding and Roaming were following a different mechanism.	3	22.2.0
36655155	NRF is not using [] in requester-plmn-list and target-plmn-list query parameters when acting as vNRF	As per 3GPP, for NFDiscover service operation, it was not clear that NRF shall encode the array of objects query attributes as array exploded way or not. When the value of `exploded` is true, NRF followed exploded way of array which meant key-value pair and repeated the same attribute for each element of array. But some operators were following the non-exploded (value of `exploded` is set as false) form of the array. It meant the array of objects need to be encoded as an array. This is applicable to NRF forwarding and NRF Roaming Cases.	3	23.4.0
36855507	oauth2 is missing correspondence between targetNfType:5G_EIR and serviceName n5g-eir-eic	AccessToken scope validation failed to accept the requests having targetNfType with underscore in the name and corresponding service names with a hyphen in the name.	3	23.4.1

Table 4-30 (Cont.) NRF 24.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
33894008	NFService level load is not used for calculating NF's load for discoveryResultLoadThreshold feature when Discovery Query is with service-names query parameter and NF Profile after filtering having one service in it.	When Discovery query had service-names query parameter with one service in it, then during load calculation, for discoveryResultLoadThreshold, NRF considered the NFService level load, if it was present, else, it considered the NFProfile level load, if present, it will use the default configured load (defaultLoad). But NRF did not consider the calculated load for **discoveryResultLoadThreshold** feature when profile load was null and there was one service with load. If **discoveryResultLoadThreshold** feature was disabled, (value as 0), this issue was not observed.	4	1.15.0
36473305	NRF - detail parameter for Error code ONRF-CFG-ACCOPT-E0021 return invalid detail response for feature	NRF returned an invalid detail parameter in the error response for the error code `ONRF-CFG-ACCOPT-E0021`.	4	24.1.0
36376682	NRF- Metric populated with method,dbOperation out of Possible values given for "ocnrf_dbmetrics_total" for feature - NRF Growth	"`ocnrf_dbmetrics_total`" metric populated the `method` and `dbOperation` dimensions even with incorrect values whereas these dimensions should be mapped with the correct values as expected..	4	23.4.0
36284356	NRF- Two Alerts OcnrfSyncFailureFromAllNrfsOfAllRemoteSets instead of one from NRF for feature - NRF Growth	NRF was generating two alerts for **OcnrfSyncFailureFromAllNrfsOfAllRemoteSets** instead of one alert with two peer sets.	4	23.4.0

4.2.7 NSSF Resolved Bugs

Release 24.2.1

Table 4-31 NSSF 24.2.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
36942926	24.1.x NSSF ocnssf_vnfd.yml has indentation issue under vnfm_info	There was an indentation issue on line #57 in the *ocnssf_vnfd.yml* file. The constraints field was incorrectly placed outside of `entry_schema` and needed to be nested within it.	3	24.1.1

Table 4-31 (Cont.) NSSF 24.2.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
36975639	ocats-nssf-24.2.0.tar has critical CVE-2024-43044	The *ocats-nssf-24.2.0.tar* had critical CVE-2024-43044 issue.	3	24.2.0
37098138	NSSF 24.1.1- Peer & PeerSet Default config with Relevant NF example and mode	NSSF guide had missing details on `configMode` for SBI configuration, specifically the HELM and REST modes.	3	24.1.1
37165977	NSSF 24.1.0 | NSSF Response code for REST API with empty configurations.	In the NSSF REST API documentation, it was specified that the expected response codes for queries like *"/nnssf-configuration/v1/plmnlevelnsiprofiles*" (amf set, Default Configured SNSSAI, NSS Rule) should be 201 or 400. However, a 404 response code was also being returned when there is no configuration found, which is typically reserved for incorrect URI paths. Clarification was requested on whether the 404 response is expected behavior for these NSSF REST APIs, or if it should align with the 200 response pattern used by other APIs.	3	24.1.0
37166035	NSSF 24.1.0 | producerScope parameter value	The function of the `producerScope` parameter in the *ocnssf_custom_values.yaml* file was unclear, as the installation guide lacks a detailed description. There was a discrepancy between the User Guide and Installation Guide regarding its correct value: User Guide: `producerScope: nnssf-configuration,nnssf-nsselection,nnssf-nsavailability` Installation Guide: `producerScope: nnssf-configuration`	3	24.1.0
36903850	Documentation needed on IGW/EGW Common Configurations	The REST API Guide and User Guide had missing detailed descriptions for Ingress Gateway and Egress Gateway route configurations and error criteria parameters.	4	24.1.1
37096524	nfSetIdList is missing in the NSSF appProfile for NRF registration	The `nfSetIdList` parameter was missing from the *ocnssf_custom_values.yaml* file.	4	24.1.0

Table 4-31 (Cont.) NSSF 24.2.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37101044	NSSF ATS 24.2.0: Change “Featues” to “Features” in the ATS console log.	In the NSSF ATS regression console log output, a spelling error was observed in both the 1st rerun section and the final result. The word "Featues" was incorrectly spelled and should have been "Features".	4	24.2.0

Release 24.2.0

Table 4-32 NSSF 24.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
36561692	NSSF should support the its own NF Instance ID for aud field in Oauth Access token.	According to the requirements, NSSF should validate the 'aud' field in the OAuth access token against its own NF Instance ID or NF type. If this validation fails, the NSSF should reject the request and respond with a 4xx error.	2	24.1.0
36595903	NSSF 3 Site GR Setup : Oauth Enabled: 2 Site Failover : 0.451% traffic loss observed for 10.5K performance run.	The user observed OAuth "Validation failure" in nsselection and nsavailability scenarios due to token validation issues, which caused a 0.072% drop in NSSF success rate during a traffic run on site-1.	2	24.1.0
36372502	ocnssf-appinfo service is not displaying or editing in CNCC's Logging Level Options.	CNC Console did not display the log level for the ocnssf-appinfo service and lacked the option to update the log level for this service. As a result, both viewing and editing the log level for the ocnssf-appinfo service were not possible within CNC Console, impacting the ability to manage logging configurations effectively.	3	24.1.0
36372109	Rest API of NSSAI Auth for plmn, tac, tac range, and network slice are not updated for PUT Method and CNCC UI.	NSSF backend function did not update the values, displaying inaccurate data for the CNC Console user. When the value was not updated, the system should have sent a failure notification, which did not happen.	3	24.1.0

Table 4-32 (Cont.) NSSF 24.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
36277930	If User-Agent Header is invalid, NSSF (HTTPS enabled) should not add the LCI and OCI Header.	When the AMF included an invalid User-Agent header in its nsselection request, NSSF responded with the LCI and OCI headers, although it should have omitted them due to the invalid peer information. Both Perfgo and NSSF had HTTPS enabled in the setup.	3	23.4.0
36277891	If the Via Header is invalid, NSSF (HTTPS enabled) should not send the failure response.	When AMF sent an invalid header in a nsselection request, NSSF incorrectly responded with an error. Instead, NSSF should have sent a successful response without the LCI and OCI headers. The issue occurred both with HTTPS and HTTP requests, resulting in either a 500 internal server error or a 403 Forbidden error, respectively.	3	23.4.0
36429909	After rollback each site, ns-availability put and patch scenarios fail with the error "Data truncation: Out of range value for column 'id' at row 1".	After rolling back each site, nsavailability PUT and PATCH scenarios failed with the error "Data truncation: Out of range value for column 'id' at row 1". The issue was encountered during in-service upgrade rollback with 1.25K traffic on both sites. The cnDBTier was skipped during the rollback due to a replication channel break issue.	3	24.1.0
36652858	NSSF Should reject Patch Replace for adding TaiRangeList which is already subscribed.	NSSF did not reject a PATCH replace operation when the *TaiRangeList* being added was already subscribed. This resulted in multiple subscriptions for the same entry, which is not the expected behavior.	3	24.1.0
36543159	"Multiple PLMN Support" : Counter value not updated while subscription rejected due to unsupported PLMN	When a subscription request was rejected due to an unsupported PLMN (Public Land Mobile Network), the counter *ocnssf_nsavailability_unsupported_plmn* was not updated. This discrepancy affected monitoring and analytics as the counter value did not reflect the actual number of unsupported PLMN subscription rejections.	3	24.1.0

Table 4-32 (Cont.) NSSF 24.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
36629839	In the ns-selection response, NSSF is sending the wrong targetAmfSet if candidateResolution is false.	During the nsselection response, the NSSF incorrectly sent the targetAmfSet "310-14-null-null" when the candidateResolution feature was disabled (candidateResolution: false). Thus, AMF could not process registration requests due to the incorrect targetAmfSet received from NSSF.	3	24.1.0
36532498	If request is received without key-Id field in access token, NSSF shall reject the service requests With ASM	When a request was received without the key-Id field in the access token, the NSSF failed to reject the service requests as expected, despite being configured in *Key ID based ONLY* mode.	3	24.1.0
36543038	"Multiple PLMN Support" : Subscription should get rejected while unsupported PLMN in subscription request , Validate cause value as well	Subscription requests with both supported and unsupported PLMNs were not rejected by the system as expected. Normally, the system should reject any request that includes unsupported PLMNs to ensure everything runs smoothly.	3	24.1.0
36515190	NSSF 23.4.0 - NSSF configuration API available through IGW External IP address	During ATP testing, it was observed that REST API commands related to NSSF configuration were accessible through the NSSF Ingress Gateway External IP. This issue was reproducible in other environments, including a local TAC lab.	3	23.4.0
35846922	Egress pod is not updating with the Entry done in DNS server "DNS SRV Based Selection of SCP in NSSF"	When an entry was added to the DNS server for "DNS SRV Based Selection of SCP in NSSF," the egress gateway pod was not reflecting this update. This prevented the egress gateway pod from correctly utilizing the updated DNS information for its operations.	3	23.3.0
36282610	Multiple Subscription Happening while configuring single AMF SET	Multiple subscriptions were being created while configuring a single AMF set in NSSF.	3	24.1.0
36548362	Multiple PLMN Support Wrong error code while Availability put reject due to unknown plmn	During an Availability PUT operation, the system was supposed to reject the request with a specific error code (403) while encountering an unsupported PLMN. However, instead of returning the expected error code, NSSF erroneously returned a status code of 400.	4	24.1.0

Table 4-32 (Cont.) NSSF 24.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
36624673	By adding any amf-set failure scenario, the metrics ocnssf_discovery_nrf_tx_failed_total are incremented twice.	The metric *ocnssf_discovery_nrf_tx_failed_total* was being incremented twice on encountering any AMF-set failure scenario, which is not the expected behavior.	4	24.1.0
36271239	The ERROR message is being printed by NSSF for NF Scoring Calculation but NSSF is not supported the NF-Scoring feature	The NSSF application encountered an error related to NF Scoring Calculation, despite not supporting the NF Scoring feature. The error message was logged during periodic updates of NF Scores.	4	23.4.0
35986423	Both IGW pod protection and overload feature enabled, NSSF is not clearing the overload alerts when overload feature disabled in runtime.	When the Ingress Gateway Pod Protection and Overload Control features were enabled in the NSSF setup, the system failed to clear overload alerts after the Overload Control feature was disabled using a curl command.	4	23.3.0

4.2.8 OCCM Resolved Bugs

Table 4-33 OCCM 24.2.3 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37779897	Incorrect alert expression in alert OccmMemoryUsageMinorThreshold	An alert was raised due to incorrect alert expression.	3	24.2.0

OCCM 24.2.2 Resolved Bugs

OCCM 24.2.2 is a Critical Patch Update. Critical Patch Updates provide security patches for supported Oracle on-premises products. They are available to customers with valid support contracts. For more information, see Critical Patch Updates, Security Alerts and Bulletins.

Table 4-34 OCCM 24.2.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36925470	OCCM ConfigMap backup with latest build must be taken before rollback to older build as certificates/Issuers created with latest build can be restored if re-upgrade need to be done to latest build after rollback.	Use the OCCM ConfigMap backup with latest build before rollback to the older build. The certificates or issuers created with latest build can be restored if upgarde is perfomed to the latest build after rollback.	4	24.2.0

Table 4-34 (Cont.) OCCM 24.2.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36915564	OCCM 24.2.0 helm test fail - Missing network policy	The Helm test failed due to incorrect network policy version.	3	24.2.0

Table 4-35 OCCM 24.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36670231	OCCM Console network policy incomplete	The allow-ingress-from-cncc-pods Network Policy was updated to include OCCM port in the `occm_network_policy_custom_values_<version>.yaml` file.	3	24.1.0

> **Note:**
>
> Resolved bugs from 24.1.0 have been forward ported to Release 24.2.0.

4.2.9 OCI Adaptor Resolved Bugs

Table 4-36 OCI Adaptor 24.2.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37012949	Management-agent pod is not coming up	Management-agent pod was not coming up while deploying the OCI Adaptor.	1	24.2.0

OCI Adaptor Release 24.2.0

There are no resolved bugs in this release.

4.2.10 Policy Resolved Bugs

Table 4-37 Policy 24.2.6 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37771658	Multiple PRE pods restarted in Sanda site	The existing process for CRUD operations on Managed Objects resulted in inefficiencies due to high memory consumption. Whenever a CRUD operation occured, the entire cache was sent to the worker nodes leading to excessive data transmission and resource usage.	2	23.4.7
37777714	Calls failing when calls made on HOLD	When the configuration server and PRE pods were restarted during a performance run, some of the PRE pods failed to evaluate.	2	24.2.3
37797575	sos failure while subscriber put normal Volte call on hold and dialed sos	The raceModerator check was unable to detect race conditions when multiple rx/sd sessions were active on the same gx session.	2	23.4.9
37824008	PCF 23.4.9 not initiating Rx RAR causing SOS call failures	PCF was not initiating Rx RAR which caused SOS call failures.	2	23.4.9
37839942	PCF 23.4.9 initiating incorrect Rx RAR causing SOS call failure || Event-trigger collision	The ACCESS_NETWORK_INFO_REPORT and/or RAN_NAS_Cause event triggers were assumed to be present if any of the fields related to the event trigger were present in the CCR-U request.	2	23.4.9

Table 4-37   (Cont.) Policy 24.2.6 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37668611	POD are taking high time to come UP during complete shutdown	PRE created many new connections towards configuration server resulting in loss of memory and pods took longer time to come up.	2	24.2.2
37694554	PCF 23.4.6 : ColoradoSprings SM-PCF 003 Diam-connector Timeouts	For diameter connector, the TCP connection was not sending any request for approximately an hour. On investigation, it was found that, TCP connection had consumed all the streams.	2	23.4.6
37883614	UDR w2 showing suspended in the PCF discovery even though it is registered fine at the NRF	The system threw an exception of not returning an unique value as it expected only one record in the case of duplicate entries.	2	24.2.3
37917657	nfscoring: 'Signalling Connections' factor's value limit not upto the mark	After enabling the NF scoring feature, the value of the Max Connection parameter was crossing the maximum possible value set as 100.	3	24.2.3

Table 4-38   Policy 24.2.5 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37642711	5G Volte call failing due to incorrect "packetFilterUsage" value in SMF notify	The `setPacketFilterUsageToTrueForPreliminaryServiceInfo` parameter was not set appropriately in the "pcf.smservice.cfg" configuration.	3	23.4.7

Table 4-38   (Cont.) Policy 24.2.5 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37726342	Incorrect log level for successful session audit attempt (RAR)	The log level for the result code DIAMETER_SUCCESS (2001) displayed WARN instead of DEBUG or INFO.	3	24.2.4
37839547	One of the Policy Projects screen not working with Policy 24.2.4 and CNCC 24.2.2	One of the Policy Projects screen was not working with Policy 24.2.4 and CNCC 24.2.2.	3	24.2.2

Table 4-39   Policy 24.2.4 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37514462	sos call failure as Rx RAR is not initiated	When the Bulwark service was disabled on PCRF-Core, race conditions for CCR-U occured against the AAR-I and Gx RAR operations. There was no mechanism to delay or retry the request.	1	23.4.7
37741240	Metrics changes due to "OCNGF-56405: AM - Productisation/Optimisation of POC Code (AUT/Contract , ATS)"	For AM and UE services, the `http_server_requests` metric has been replaced with `occnp_amservice_overall_processing_time` and `occnp_ueservice_overall_processing_time`, respectively.	2	24.2.4
37417501	All nrf-client Discovery pods restarted at Rocklin site due to out of memory	Traffic was impacted when all the NRF Client pods were restarted due to out of memory.	2	23.4.4

Table 4-39 (Cont.) Policy 24.2.4 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37422744	Observed 500 Internal Error due to Audit Notifications	Egress Gateway pods came up before the Alternate Route Service (ARS) pods and failed to resolve the SCP FQDN. ARS lookup query returned 503 response.	2	23.4.4
37617921	Veriyfying congestion Control on bulwark over 75K TPS leads to > 50% Traffic Drop happen and did not recover	In an ASM-enabled setup, when the Bulwark pod was in a congested state and the default response was set to 503, unsolicited retries were processed at ASM on all the 503 requests.	2	24.2.1
37547053	ARS responding with "did not accept task"	Alternate Route Service (ARS) had issues while processing requests from backend services. ARS rejected registration and lookup requests due to improper thread pool configuration.	2	24.2.4
37581310	Diameter Connector Not Processing AAR response reject message	The Diameter Connector did not process AAR response reject message.	2	24.2.2
37617119	Diam-Gateway pod restart observed due to OOM on Policy	During the Diameter request timeout, the Diameter Gateway printed logs which consumed complete container memory resulting into pod restart.	3	24.2.4

Table 4-39 (Cont.) Policy 24.2.4 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
7639009	Error DB task Exception caught {}",localizedMessage":"expect '{', but '\u0012', offset 1, character \u0012, line 1, column 2 observed while the traffic is running and PDS application compression is being enabled	There were multiple error logs in the PDS. These errors occurred when the compression flag was modified for an in-flight message.	3	24.2.4
37643986	Scaling Down All Config server Replicas leads to Traffic failure and Drop in success rate in AM and UE call Model	Scaling down all the config-server replicas lead to traffic failure and drop in success rate in AM and UE call Model. When the config-server encountered an error, PRE sent an empty response.	3	24.2.4
37470144	clsp and rckl observed to have AMF-PCF and UE-PCF failures	Although the **UE Communication Profile** used for sending callback header was enabled in the CNC Console, UE service was not sending "3gpp-sbi-callback" header to AMF as part of Update Notify request for user data change. As a result, SCP was trimming callback portion of the URI resulting in 500 INTERNAL_SERVER_ERROR.	3	23.4.4
37494114	PCF Duplicate 3gpp headers issue for SM and AM	SM, UE, and binding services were sending duplicate 3gpp header values.	3	23.4.2
37516856	Importing data from 23.4.4 to 24.2.3_OCNGF-67648 it seem nrf_agent config are lost	During data import with the ignore flag, the config-server incorrectly considered the empty JSON as valid configuration data.	3	23.2.4

Table 4-39 (Cont.) Policy 24.2.4 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37487698	PCF UE Policy NAS Retry Profile exports Default Value	UE service configuration did not return the NAS related attributes through Rest API.	3	24.2.2
37513871	East-AMPCF 000 / 002 EnableData Compression post change DC log collection	AM service logs were full of parsing errors for the "SERVICE_NAME" binding parameter.	3	23.4.4
37415315	PCF Undeploy/delete failed with Error	PCF uninstallation workflow failed with error.	3	24.2.2

Table 4-40 Policy ATS 24.2.4 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37630726	BindingCreation_AsynchronousMode_global test case failing in regression	The BindingCreation_AsynchronousMode_global test case failed during regression.	3	24.2.4

Table 4-41 Policy 24.2.3 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37207883	SOS Call is not working when subscriber is in KDDI PLMN	When CCR-U came with UserLocationInfo with GeographicLocationType equals to 130, mcc-mnc of the *TrackingAreaIdentifier* was kept but the mcc-mnc of the *EUTRANCellGlobalIdentifier* was lost and used the one in the TAI, saving only one mcc-mnc in the database. This mcc-mnc was sent to Rx RAR in both the TrackingAreaIdentifier and EUTRANCellGlobalIdentifier AVPs.	1	23.4.5

Table 4-41 (Cont.) Policy 24.2.3 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37450445	Policy Variation of "When leader diam-gateway pod goes down, stale entries in distributed cache cause IPR to fail due to NPE"	When the Diameter Gateway leader pod went down, the entries remained stale in distributed cache. But, while iterating through those entries for inter-pod routing, Diameter Gateway worked in NPE. This caused message routing failure.	2	24.2.3
37453470	PCF respond Sy SNA with error code 5012 (Diameter_unable_to_comply)	On CCR-I, SLR-Initial/Intermediate was sent to OCS and it responded with error code 2001 without any policy counters. After some time, the policy counters for the subscriber were provisioned and OCS sent SNR along with the policy counters. The SNR was failing and responded with error code 5012.	2	23.4.7
37228756	CHIO and INDE :Timeout exception occurred while sending notification request to Notification Server	Whenever a server was closing a connection or the server was restarted, then there was a proper handling of connection cleanup through Jetty callback method to clean up the connection count and the connection itself.	2	23.2.0

Table 4-41 (Cont.) Policy 24.2.3 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37234682	Prod SMPCF: SQLException on put (24.2.3)	On RAR/ASR processing if AppSession was not present in database, the action was cancelled and no cleanup to AppSessionInfo was made. It caused the stale appSessionInfos and related pcc rules to stay alive in the SmPolicyAssociation which overloaded the session beyond the allowed size limit in the database.	2	23.4.5
37214196	PCF is not responding udr delResources notification for SM Policy	There was a NPE while retrieving the service name after a UDR notification with delResources was sent. It resulted in PCF is not responding udr delResources notification for SM Policy.	2	24.3.0
37219012	PCF 24.2.x Bulwark POD creation error in ATS Lab with WS 1.5	The bulwark pod was not starting due to file permission issue.	2	24.2.1
37208887	MPCF - Policy Evaluation Failure	As config data cache maintained in Policy blockly takes only higher version, the cache was not updating in case of snapshot as snapshot keeps old or lower version.	2	23.4.6

Table 4-41 (Cont.) Policy 24.2.3 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37245151	For N7 session failure due to policy decision, PCF not sending UDR unsubscribe for 2nd DNN, will cause stale sessions on UDR. (24.2.3)	When create request was rejected after sending request to PDS and UDR, SM service triggered unsubscribe request to PDS. Since PDS did not receive response from subscribe from UDR, it does not send unsubscribe request to UDR leaving a stale session in UDR.	2	24.2.0
37292302	Usage Monitoring - Making MK AVP optional for Session Level Grant	Usage-Mon was always sending monitoring key in CCA.	3	24.2.3
37307794	Policy variation of bug "TWBG prod Post BSF upgrade Over load congestion	High CPU utilisation was observed when BSF was upgraded to 23.4.4.	3	23.4.6
37348507	Policy is sending Incorrect ETAG value in PATCH after receiving Notification from UDR for Provisioning Update	UDR was generating a notification and sending an updated eTag, but it was not storing as per the current implementation.	3	24.2.3
37440133	PCF Undeploy/ delete failed with Error	PCF delete workflow failed with an error.	3	24.2.3
37447641	SESSION_LEVEL quota is allocated even though the base data limit profile is PCC_Level	SESSION_LEVEL quota was allocated even though the base data limit profile was PCC_Level. As UMLevel is set from umData and not from the base data limit profile, so the PCC_LEVEL quota was not being allocated.	3	24.2.3

Table 4-41 (Cont.) Policy 24.2.3 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37307043	Call failure - 503 service unavailable	On SmRx call flow with ACCESS_TYPE_CHANGE AfEvent on AAA/RAR when ratType did not have the supported values from 16.3 (NR, EUTRA, WLAN, and VIRTUAL), diam-connector was unable to translate triggering 5012 AAA responses/ 500 RAA responses.	3	23.4.4
37297031	Observing "json.decoder.JSONDecodeError" in Performance pod of PCRF application	There was JSON.decoder error while loading data from cgroup.json file.	3	23.4.0
37219286	Monitoring quota consume in a excess usage scenario - Granting Quota	If excess usage was enabled after CCR-T and CCR-I for the same subscriber came, usage-level became negative and CCR-I was sent in umPolicyDecision towards pcrf-core. Also, the negative usage-level value is going towards PRE.	3	24.2.1
37212599	cnPCRF Rollover MK incorrect name	Usage-Mon ws not allowing to have multiple plans with same monitoring key. It required unique monitoring key based on 3GPP 29.512.	3	23.4.0
37207796	Alerts are not patching in Prometheus and Alert Manager	Improper Alerts indentation in the YAML file caused the error while applying the alert file.	3	24.2.1
37142733	Audit service not working with 2 Replicas	The Audit service was not working with two replicas.	3	24.1.0

Table 4-41 (Cont.) Policy 24.2.3 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37148539	Set Grant Time blockly does not work when you use a dynamic variable and select Duration	The "Set Grant Time" blockly did not work while using a dynamic variable and selected duration.	3	24.2.1
36727061	Issue updating Subscriber State Remote Variable	On Gx CCR-U processing, PCRF-Core project specific variables were overridden by Usage Monitoring (UM) variables and only state variables of UM were sent to PDS.	3	23.4.2
36928821	Usage-monitoing pod logs are not included in the Subscriber activity log	PCRF-core service was not forwarding subscriber headers towards usage-mon whenever Subscriber Activity Logging (SAL) was enabled for Gx session.	3	23.4.3
37043367	Sy-SLR is failing at diam-gateway with 5012 error-code due to subscriber-activity-logging error	CM Service was wrongly creating the mapping entries in database matching the existing SmAssotiationIds as it was using the ENUM name instead of ENUM value as key.	3	24.2.1
37224279	CHIO cnPCRF, POD restarted chio-cnp-cnpcrf-notifier	All the notifier pods were restarted at both the sites as per the chio-cnp-cnpcrf-notifier log.	3	23.2.8

Table 4-42 Policy ATS 24.2.3 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37374884	Faliure observed in "User_Agent_Policy_Propagation" Feature	This is a timer issue as the previous feature file having some Model D related cfg changes and this was reverted during scenario cleanup and it takes almost 40s to complete it and till then the next scenario run and it got impacted by the above configuration.	3	24.3.0
37215643	Bulwark_Support_SM_Create_Delete_UpdateNotify_PDSNotification_RedCap_ocLog failing	"Bulwark_Support_SM_Create_Delete_UpdateNotify_PDSNotification_RedCap_ocLogId_verify" and "Non_SUPI_ODD_Caching_AM" were failing due to incorrect configurations.	3	24.2.1
37228254	NRF_Error_Response_Enhancement_PCF_as_Producer failure in NewFeature	The FQDN 'occnp-ocpm-ingress-gateway.rcnltxekvzwcpcf-y-or-sm-008.svc' name was truncated which caused failure during validation.	3	

Table 4-43   Policy 24.2.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37217210	PCF 24.2.x Bulwark POD creation error in ATS Lab with WS 1.5	Prior to 24.1.x, Bulwark service pods included folders, subfolders, and files within `/opt/oracle` with access permission `777`. Post 24.1.x, the access permission for all the folders, subfolders, and files were changed to 544 due to security concerns. This resulted in denial of access to any group and user, other than `pcf:pcf:(5000:5000)`, to execute the shell scripts within this folder, particularly `/opt/oracle/docker-entrypoint.sh`. This access issue caused Bulwark POD creation error in ATS Lab.	2	24.2.1

Table 4-44   Policy 24.2.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37039691	In PCF R23.4.5 IGW is strict in requiring content-length header on POST/PUT/PATCH when a body is present	When a request body is present in the request received, the content-length header should be present in the POST, PUT, or PATCH request.	2	23.4.5

Table 4-44   (Cont.) Policy 24.2.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36878972	NullPointerException From IGW for GET pending-req-count	A NullPointerException was observed whenever GET "/igw/pending-req-count" was called, resulting in 500 error. It happened while fetching an entry from coherence pending-req-count cache did not result in any value. This unavailability of the data from coherence cache was not handled gracefully resulting inNullPointerException.	2	23.4.6
37080665	Huge logs are flooding as "Exit requested from Policy evaluation" due to end all blockly	Multiple "Exit requested from Policy evaluation, hence Exiting from policy" message was getting logged at WARN logging level unnecessarily.	2	22.4.4
36960476	RAR messages not being generated on gx	MatchList blockly was not working with "create list with" value (left side). The removal of third-party library called Lodash had caused these issues.	2	24.2.0

Table 4-44 (Cont.) Policy 24.2.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36884531	PCRF performance run observed Binding serv error "Invalid compressed data" & "No content to map due to end-of-input\n at [Source: (String)\"\";	This issue was observed because the JDBC 'characterSetResults' was defaulted to UTF-8 in the Binding service. Due to this, the byte array before compression and after decompression was not same and caused invalid end of inputs. This setting is now removed from JDBC URL in the Binding service.	2	24.2.0
36871120	PCF sending error 415(UNSUPPORTED_MEDIA_TYPE) for policyauthorization delete request is missing header content-type	Default content-type header with value "application/octet-stream" was added by Ingress Gateway to the POST request before sending to backend without a payload.	3	23.1.2
37019998	Queue and CPU values cant be set to zero for bulwark service under congestion control thresholds page in PCF GUI	In the prior releases, the suggested way to disable the Bulwark congestion control was to set the CPU and Queue size values to "0" through PCF GUI. But, the PCF GUI was not accepting "0" value for the configurations.	3	24.2.0
37058323	STR is not sent by PCF if CCA-I sent with error code	On CCR-I when PRE rejects or releases the request, PDS unsubscribe was not sent to cleanup PDS GET that happened before. Now, if any error cancels the request on CCR-I proper PDS unsubscribe will be triggered if needed.	3	23.4.5

Table 4-44 (Cont.) Policy 24.2.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37090621	UMservice to PCRF Core Negative Grant Value is being sent.	When duration field of Excess Usage Limit was left empty, it was throwing null pointer exception and provided incorrect grant request.	3	24.2.0
36977245	Block "Contained in matchList" doesn't work	MatchList block was not working with "create list with" option.	3	24.2.0
36988635	SM latency getting increased resulting in rx traffic discard beyond 43K (New call Model)	When diameter connector sent HTTP requests to SM and PDS, the request and response were processed in the context of jetty threads. Jetty threads were limited in number and not meant to be configured for performance heavy tasks. Therefore, threads were running out and blocking incoming requests.	3	23.4.5
37000834	Minor Limitations on ExcludeDNN Functionality	On SM call flows, PRE was able to trigger SSV Update even if excludeDNN was enabled for PDS.	3	23.4.5

Table 4-44 (Cont.) Policy 24.2.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36938337	CV files for GW's should be updated for maxConnectionsPerDestination, serverDefaultSettingsMaxConcurrentStream and requestCountSamplingInteval configurations	`Custom_values.yaml` file was missing the following ingress and egress gateway configurations which are present in gateway level chart values: • nettyInboundExceptions • serverDefaultSettingsMaxConcurrentStream • requestCountSamplingInteval The default value for `maxConnectionsPerDestination` parameter has been changed from 10 to 20.	3	23.4.5
36991926	SM create requests are not rejected when sm pod moves to DOC state with discard priority 20	SM service was not taking the new configuration change while creating and activating a custom load shedding rule.	3	24.2.0
36888683	Warning message "ProducerId Header is Not present in BSF Response"	In binding pods logs were flooded with a WARN level message "ProducerId Header is Not present in BSF Response".	3	23.4.4
36928734	QOS parameter : Max DataBurstVol" is taking values between 1-4065 and not 0 or null	The correct range specified for MaxDataBurstVol was between 1 to 4095 with default value of 2000. It was not accepting the null value.	3	24.1.0
36875568	Monitoring quota consume in a excess usage scenario - customer query	Usage-Mon was not sending consumed quota with excessUsage added in base quota, resulting in wrong calculation.	3	23.4.0

Table 4-44 (Cont.) Policy 24.2.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36909037	PRE performance degradation when using MatchList in Policy Table	Usage Monitoring policy with MatchList in Policy Table was causing high latency and high CPU usage for PRE microservice. One of the (Array) data structures used to store the data while using this blockly was not getting cleaned up. It kept accumulating data in it and over the time was slowing down the performance and increasing the latency.	3	24.2.0
36181369	PCF does not respond with error code configured in blockly towards SMF/AMF for error response received (401 UNAUTHORIZED with cause WWW-Authenticate) from UDR for GET request	Backend services (SM/AM/UE) were not adding the required header (WWW-Authenticate) in the response which was needed by Ingress gateway to respond properly.	3	23.2.0
36978657	Set Grant Volume blockly does not work when you use a dynamic variable and select bytes	The "Apply Data Limit Profile" blockly with set volume Grant option was not working when used with Bytes in place of percentage.	3	22.4.7

Note:

Resolved bugs from 24.1.x and 24.2.x and have been forward ported to Release 24.2.1.

Table 4-45 Policy 24.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36262892	Observing PCF Sending wrong Policy triggers during call Hold	PCF was sending incorrect policy triggers such as AC_TY_CH and AN_INFO during a call hold scenario.	2	23.4.0
35910173	Redendancy_Testing_Got_failed_for_SM_service	Redundancy test failed for SM service with 400, 408, 500, and 503 errors.	3	23.1.3
36179862	New Protocol Data Unit (PDU) session using stale CHF data	New PDU session updated with imsi 311480039666027 used stale data from previously terminated session.	3	23.2.6
36396992	System misbehavior at 23k / 30k TPS	Multiple errors and exceptions were observed when PCF crossed 21K TPS.	3	23.2.7
35871742	PCF 23.2.2 Lab Error code sorting does not allow to update or delete error objects	Error code sorting does not allow to update or delete error objects.	3	23.2.2
35828884	cm-service: Could not find the config for requested service	Configuration service could not find the configuration for the requested service. Errors persisted even when the Audit service was disabled.	3	23.2.1
36382943	PCF voice call issue with PolicyDS	Issues were observed with voice call when the PDS pod was disabled.	3	23.4.1
35784101	SMservice Reject message with SESSION_NOT_AVAILABLE when request has framedip-IPv6	SM service displayed `SESSION_NOT_AVAILABLE` message when the incoming request had framedip-IPv6.	3	23.2.1
36045264	PCF Sending ASR for sessions that have already ended	ASR was sent after responding STA with 2001.	3	23.2.4

Table 4-45 (Cont.) Policy 24.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36727451	PCRF not managing passes correctly	Pass to control the expiration date and the consume status are defined in UDR so when the date is expired or the Pass is exhausted, PCRF should send an update to the UDR and remove it. But, PCRF retrieved it from the UDR and did not grant the MK for this pass. Instead, PCRF granted the base quota.	3	23.2.0
36023067	PCF GUI Import Policies not showing up the correct values after the import	After the bulk import using CNC console, the values for one of the sub policies(NudrDynBlobWrite_037) were not available on blocky code.	3	23.2.5
36422005	23.4.0 cnPCRF rollover monitoring key has incorrect name	When data rollover is enabled, the prefix in the monitoring key name was not the one defined in the DataLimitProfile.	3	23.4.0
36497882	SCP Route blacklist duration is not working as expected	SCP Route blacklist was not working as expected. PCF received 503 from SCP1. PCF blacklisted SCP1 and rerouted to SCP2. Again PCF sent the next message to SCP1 even before the blacklist.duration timer (60second) expired.	3	23.2.2
36566643	Incorrect Encoding of the MNC Value in URSP Policy	PCF was sending the MCC MNC values as a part of the URSP Policies in Manage Policy UE Command.	3	23.4.1

Table 4-45 (Cont.) Policy 24.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36415837	Rx-STA-5063 failures observed during the 10hr performance run	After overload configuration was modified, STR responses resulted in ERROR-5063 (REQUESTED_SERVICE_NOT_AUTHORIZED).	3	22.4.7
36412979	cnPCRF 23.4.0 Session NextBillingDate not available	To migrate 4G legacy policies to cnPCRF, there was no blockly where based on the BillingDay store on the profile of the cnUDR, NextBillingDate timestamp could be retrieved.	3	23.4.0
36232668	PolicyDS responds to SOAP-NOTIFY with previous LDAP data when the PDS profile is updated correctly	PDS responded to SOAP-NOTIFY with previous LDAP data when the PDS profile was updated. The INFO logs from PDS contain the old PDS data in the SERVER_RESPONSE.	3	23.2.4
36294326	PCF - Getting alert for "altsvc-cache" with alternateRouteService disabled	Alerts for altsvc-cache were observed even though they were disabled.	3	23.2.4
36544216	PCF Duplicate 3gpp headers issue for SM and AM	Duplicate 3GPP headers were observed for SM and AM services.	3	23.4.2
36508175	Sometime RAR is not triggered to PGW when SNR from OCS for QOS changes	When SNR request was received to change the QOS information, PCF did not send the RAR towards PGW to change the QOS information .	4	23.4.0

Table 4-45 (Cont.) Policy 24.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36727396	PCF AM-001 EGW 503 ERRORS	503 UF `upstream_reset_before_response_started{connection_failure}` errors were observed at Egress Gateway.	4	23.4.3
36437298	RX and Binding sessions do not match	After enabling the Binding service (BSF) the total number of RX sessions and the total number of binding sessions did not match.	4	23.2.4
36777422	Same session ID is triggered by PCF for different subscriber - Sd interface	5012 errors were observed for TSR/TSA message in Sd interface when the same session ID was triggered by PCF for different subscribers.	4	23.4.0
36786330	All Data Limit Profiles are sent to the PRE microservice	All Data Limit Profiles were sent to PRE when experimenting with quotas. This could significantly impact the microservice's performance when there are numerous Data Limit Profiles.	4	23.4.3
36727466	PCF sending incorrect NCGI format in Rx RAR to CSCF	In Rx RAR message, the MCC/MNC part of the NCGI value within 3gpp-user-location-info header was incorrectly formatted. During decode process, the value obtained was in bad format.	4	23.4.0

Table 4-45 (Cont.) Policy 24.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36817637	SM PCF egress traffic failing after 23.4.2 Upgrade	After upgrading to Policy 23.4.2, Egress Gateway failed to send outgoing traffic towards SMF, UDR, CHF, and BSF.	4	23.4.2
36727430	Post upgrade to 23.4.3, Policy Create, Policy Update and Policy Delete have error 403 Forbidden	Following issues were observed after upgrading to Policy 23.4.3: • Ingress Gateway experienced 403 errors. when it received SM CREATE, SM UPDATE, and SM DELETE requests. • UDR connector encountered 403 errors when sending a PUT request for a subscription.	4	23.4.3
36732517	PCF PRE Pods are getting restarted on 80% Load	PRE pods were getting restarted on 80% load capacity. Prometheus memory graph indicated that PRE pods memory reached 100% before their restart.	4	23.4.0
36473056	Rx Authorization Authentication Requests (AAR) failing with 5065 since signalling storm at 11/03 00:10	When there was a spike in the Gx and Rx traffic, around 15% of AAR responded with 5065(IP-CAN_SESSION_NOT_AVAILABLE).	4	23.2.4
36741578	SM PCF site was affected due to Memory utilization	Memory limits hit on CSP SM-PCF, responding with timeouts. This affected the functioning of the site.	4	24.2.0

Table 4-45 (Cont.) Policy 24.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36782042	SM-PCF sending nUDR subs-to-notify with two monitoredResourceURIs in the message - resulting in N36 setup failure	SM-PCF was sending nUDR subscription-to-notify with two monitoredResourceURIs in the message , resulting in N36 setup failure.	4	23.4.3
36875630	PCF ENF_APP_Flow rule removal blockly not working	The "ENF_APP_Flow" rule removal blockly was not working in PCF.	4	23.2.4
36853396	cnPCRF 23.4.3 4G Reset Usage DataLimit action not working	The Reset Usage DataLimit action was not working in cnPCRF 23.4.3 4G.	4	23.4.3
36846987	Multiple Session Termination Request (STR) is triggered by cnPCRF towards Online Charging System (OCS) during performance testing	Multiple STRs were triggered by cnPCRF towards OCS during performance testing.	4	23.4.0
36853456	Quota grants not considering float percentage values	Usage Monitoring service stored only whole numbers in Usage Threshold (Data plan) to grant data. Based on this number, threshold percentage was also calculated as a whole number. If the calculated percentage had a decimal value, it must be rounded off.	4	23.4.3
36842175	cnPCF 23.4.0 // Egress GW removing IPv6 first hexadecimal Octet for N28 SpendingLimit request	Egress Gateway was removing the first hexadecimal Octet in IPv6 for N28 SpendingLimit request.	4	23.4.0

Note:

Resolved bugs from 21.4.x and 24.1.x and have been forward ported to Release 24.2.0.

Table 4-46   Policy ATS 24.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
36696943	PCF-ATS 24.1.0 - Regression feature failures (24.2.0)	The following features failed in the regression run due to metric mismatch: • *Discover_UDR_Using_GroupId_AM_UE* • *Discover_UDR_Using_GroupId_SM* • *Non_SUPI_ODD_Caching_UDR*	3	24.1.0
36466201	OCC Lab : PCF-ATS 24.2.0 - Newfeature failure	NRF_Error_Mapping_Autonomous_Registration feature configuration was failing in the scenario `NRF_Error_Mapping_Autonomous_NFRegister_and_NFUpdate_500_Internal_Sever_Error`.	4	23.4.1
36727101	PCF_ATS_23.4.3 - UE_stale_session_audit feature failure	`UE_stale_session_deleted_maxTTL_reached_queryAMF_request_timeout` scenario of "UE_stale_session_audit" feature was failing in regression pipeline.	4	23.4.3

4.2.11 SCP Resolved Bugs

Release SCP 24.2.4

SCP 24.2.4 is a Critical Patch Update. Critical Patch Updates provide security patches for supported Oracle on-premises products. They are available to customers with valid support contracts.

For more information, see Critical Patch Updates, Security Alerts, and Bulletins.

Table 4-47   SCP 24.2.4 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37830939	SCP rejects the traffic even when the egress rate limit is set to a higher value	While operating traffic at 730K MPS, SCP rejected the traffic even if the Egress Rate Limiting configuration was set to a higher value.	2	24.2.0
37729643	SCP not sending message to SMF	SCP could not communicate with SMF even after updating the TLS certificate.	2	24.2.1

Table 4-47 (Cont.) SCP 24.2.4 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37546329	decodeCcaHeader(): Invalid format for CCA Header, Not able to parse it	When the CCA validation header was tested, error 403: CCA_VERIFICATION_FAILURE was observed.	3	24.2.2
37830908	If 3gpp-Sbi-Target-apiRoot sent without port, SCP uses 80 by default for https scheme	When the 3gpp-Sbi-Target-apiRoot header was sent without a port, SCP used port 80 by default for the HTTPS scheme.	3	24.2.3
37830922	OCSCP Upgrade from 24.2.2 to 24.2.3 fails during scpc-notification-pre-upgrade job	SCP upgrade from 24.2.2 to 24.2.3 failed during the scpc-notification-pre-upgrade job.	3	24.2.3
37830975	nfTypeExtensionSelfValidation Error for nfTypes encoded with ASN.1 Sequence	When SCP was upgraded from 24.2.1 to 24.2.3 and the nfTypeExtensionSelfValidation parameter was set to true, an error was observed in the scp-init pod.	3	24.2.3
37674874	TLS1.3 Handshake is failing between SCP and NRF	TLS handshake between SCP and NRF failed intermittently with TLS 1.3 after idle timeout.	3	24.2.3
37830984	alternate resolution pod got restarted while traffic is running at the rate of 730K MPS	The alternate resolution pod restarted when the traffic was running at the rate of 730K MPS.	3	24.2.3
37752879	SCP still not sending total Root CA chain in server Hello TLS 1.2	During the TLS handshake, SCP 24.2.3 was sending the server Hello without the sub-certificate, which was part of the total rootCA chain. SCP only sent the SCP certificate and the root CA.	3	24.2.3

Table 4-48 SCP ATS 24.2.4 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37697605	Helm chart installation fails with PVEnabled	Helm chart installation failed when the PVEnabled parameter was set to true.	3	24.2.3

Release SCP 24.2.3

SCP 24.2.3 is a Critical Patch Update. Critical Patch Updates provide security patches for supported Oracle on-premises products. They are available to customers with valid support contracts.

For more information, see Critical Patch Updates, Security Alerts, and Bulletins.

Table 4-49   SCP 24.2.3 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37410361	SCP not adding its own FQDN as server header back to consumer from SCP during ingressRL	SCP did not add its FQDN as the server header back to consumer NF from SCP during ingressRL.	2	23.4.3
37480396	SCP-audit does hashmap for its own InstanceID results in alert NF_PROFILE_VALIDATION_FAIL	SCP-Audit generated a hashmap of its SCP NF profile instance ID after retrieving NF profile for the audit cycle.	3	24.2.1
37179011	SCP is not recovered from Circuit Breaking Condition though ingress traffic rate is reduced	SCP did not recover from the Circuit Breaking condition when the ingress traffic rate was reduced.	3	24.2.1
37480363	S1G4 SCP_DNSSRV_ProducerBasedOverloadControl_P0 110624 failing due to metric mismatch	After profile update, PeerLCI Congestion State did not update and resulted in testcase failure.	3	24.2.1
37480408	SCP 23.3.0 NF Profile Registration failed due to NF_RESOURCE_MAPPINGS table size	SCP 23.3.0 NF profile registration failed due to error in creating entries in the NF_RESOURCE_MAPPINGS database table.	3	23.3.0
37480344	SCP percent encoding in Path URI not working when mediation feature is enabled	SCP percent encoding in Path URI was not working when the Mediation feature was enabled.	3	24.2.1
37480329	Server Header - sideCarProxyStatusCode is mandatory - Bad Request	It was observed that the sideCarProxyStatusCode parameter was mandatory instead of optional.	3	23.4.3
37480317	Issue with AR when NFset followed by Static Config w/o Routing Binding header	Alternate Routing did not work when NFset was followed by static Config without the Routing Binding header.	3	23.4.2
37415813	Pod restarts when call to kubernetes API fail continuously for more than certain seconds	Pod restarted when call to Kubernetes API failed continuously for more than certain seconds.	3	24.3.0

Table 4-49 (Cont.) SCP 24.2.3 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37480290	Pod Overload control based on pending transactions has gauge metric ocscp_worker_pending_upstream_resp_count left with stale count	The Pod Overload Control based on Pending Transactions feature had gauge metric ocscp_worker_pending_upstream_resp_count left with a stale count.	3	24.3.0
37478242	SCP 24.2.2 - When an NF is registered without port, the SCP is using 80 by default for https scheme	When an NF was registered without port, the SCP used port 80 by default for https scheme.	3	24.2.2
37089798	SCP need to validate client cert from root ca to intermediate ca and also need to share the complete certs	SCP did not validate client cert from root ca to intermediate ca and also required to share the complete certs.	4	24.3.0
37517086	NF Profile default rules do not have nfstatus of nfprofile parsed correctly	NF Profile default rules did not have nfstatus of nfprofile parsed correctly.	4	24.2.2
37499976	SCP 24.2.2: Error while establishing a connection to watch secrets (DataDirectorSASLConfig)	An error occurred while establishing a connection to watch secrets (DataDirectorSASLConfig).	4	24.2.2

Table 4-50 SCP 24.2.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37226665	SCP hop-by-hop-id metadata in messages forwarded to OCNADD should be unique for messages in each hop	The hop-by-hop-id metadata in messages forwarded to OCNADD was not unique for messages in each hop.	3	23.4.0
37226666	SCP should not forward internal hop traffic to OCNADD	SCP was sending SCP's internal traffic to OCNADD because SCP was expected to send only 5G SBI messages to or from SCP.	3	23.4.0

Table 4-51 SCP 24.2.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36573176	SCP generates 429(overload) while running the mediation traffic	While running the mediation traffic at the rate of 640K MPS, SCP experienced an overload condition and generated 429 messages.	2	24.1.0
36560640	Worker pod restart observed while running the traffic at the rate 640K MPS with mediation feature enabled	SCP-Worker pod restarted while running the traffic at the rate 640K MPS with the mediation feature enabled.	2	24.1.0
36941906	SCP: After automatic/manual mode override new certificate validity is not applied by SCP worker pod.	After the automatic or manual mode override, new certificate validity was not applied by the SCP-Worker pod.	2	24.2.0
37017087	SCP 24.2.0: Model D not working when interPlmnFqdnValidationEnabled	When the interPlmnFqdnValidationEnabled feature was enabled, Model-D stopped working.	3	24.2.0
36994816	scp-worker in crashloopbackoff when 2 out of 3 K8s master are down	SCP-Worker was in the crashloopbackoff state when two out of three Kubernetes primary nodes were down.	3	23.4.1
36959196	SCP23.4.3-InterSCP Scenario - Invalid 3gpp-sbi-target-apiroot	SCP-C was unable to route the request to the target SCP because the 3gpp-target-api-root header was set to NA.	3	23.4.3
36932725	SCP 23.2.2 does not create routing rules for UDM	SCP 23.2.2 did not create routing rules for UDM.	3	23.2.2
36896318	Audit pod restarted after SCP hits critical threshold level with error rate induced	SCP-Audit pod restarted after SCP reached critical threshold level with error rate induced.	3	24.2.0
36891970	270K MPS Traffic with Message-Copy feature resulting in scp-worker restarts	When the Message Copy feature was enabled and RxRequest and TxRequest were marked for copy for configured trigger points, it was observed that the SCP-Worker pods restarted after sending 270K MPS traffic.	3	24.2.0

Table 4-51 (Cont.) SCP 24.2.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35341610	Traffic failure(429 overload discard) was observed while running traffic at 462K/512K MPS using 8vCPU as well as 12vCPU worker pod profiles	Traffic failure (429 overload discard) was observed while running traffic at 462K/512K MPS using 8vCPU and 12vCPU SCP-Worker pod profiles.	3	23.1.0
37056446	S1 of SCP_EgressCongestionBasedOnProducerLoad_AlertMessagePriority_CHF_P0 failed	The SCP_EgressCongestionBasedOnProducerLoad_AlertMessagePriority_CHF_P0 feature failed with the "ERROR! Unexpectedly Alert has been fired for Key Value Pair ocscp_peer_fqdn" message.	3	24.2.0
36866817	ocscp_metric_dashboard_promha_23.4.1.json still using old metrics which have been already renamed	`ocscp_metric_dashboard_promha_23.4.1.json` was still using old metrics that were already renamed.	4	23.4.1

Table 4-52 SCP ATS 24.2.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36999661	SCP ATS 24.2.0-OCATS pod is in "CrashLoopBackOff" state when ATS installed with ASM	During the validation of SCP 24.2.0, installation failed and the ATS OCATS pod was stuck in the CrashLoopBackOff state.	3	24.2.0
37032150	Observed 429's due to pod overload discards during upgrade from 24.1.0 to 24.2.0-rc.5	Observed HTTP response error code 429 due to pod overload discards during upgrade from 24.1.0 to 24.2.0.	4	24.2.0

Note:

Resolved bugs from 23.4.3 and 24.1.1 have been forward ported to Release 24.2.1.

Table 4-53 SCP 24.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36562257	SCP is not correctly applying the match filter when running the mediation traffic	SCP did not correctly apply the match filter when running the mediation traffic.	2	24.1.0
36659112	SCP Alternate Routing using DNS SRV not working	SCP alternate routing using Domain Name System Service (DNS SRV) did not work.	3	23.4.1
36623022	Mediation rule is not triggered when user-agent header	The mediation rule was not triggered when the user-agent header was present.	3	23.4.1
36621069	ocscp-scp-mediation-test deployment not taking serviceAccountName from Yaml	ocscp-scp-mediation-test deployment did not take the serviceAccountName from the YAML.	3	23.4.1
36575958	SCP Feature Ignore Unknown Nf Service not working for 5G_EIR profile	SCP feature "Ignore Unknown NF Service" did not work for the 5G Equipment Identity Register (5G_EIR) profile.	3	23.4.1
36572372	Alternate Routing using Static Configuration not working as expected	Alternate Routing using static configuration did not work as expected.	3	23.4.0
36566408	Unable to configure nnef-afsessionwithqos service of nef nf type under "NF Discovery Response Cache Configuration Rule"	The user was unable to configure the Nnef_AFsessionWithQoS service of NEF NF type under "NF Discovery Response Cache Configuration Rule".	3	24.1.0
36566363	Getting 500 Internal server error while configuring target nf type as 5G_EIR	The user encountered a 500 Internal Server Error while configuring the target NF type as 5G_EIR.	3	24.1.0
36547446	SCP is sending wrong status code 508 Loop detected when it receives request without discovery headers and neither it has 3GPP-Sbi-Target-apiroot and 3GPP-Sbi-Routing-Binding headers.	SCP sent the wrong status code 508 Loop Detected when it received a request without discovery headers, and it did not have the 3GPP-Sbi-Target-apiroot and 3GPP-Sbi-Routing-Binding headers.	3	24.1.0

Table 4-53 (Cont.) SCP 24.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36532874	scp is responding 400 with an unclear error detail when we try PUT api on NF Profile	SCP responded with a 400 error with unclear error details when attempting to PUT API on NF Profile.	3	24.1.0
36526885	scp-worker not including query parameters when mediation rules is applied	SCP-Worker did not include query parameters when mediation rules were applied.	3	23.4.1
36489251	REST API PUT request validation needs to be corrected for NF Discovery Response Cache Configuration	The REST API PUT request validation required correction in NF Discovery Response Cache Configuration section.	3	24.1.0
36453501	SCP is not sending absolute URL towards consumer in case of producer includes slash("/") in location header	SCP did not send absolute URLs to the consumer when the producer included a slash ("/") in the location header.	3	24.1.0
36441208	SCP Health Check feature clarifications	Clarifications regarding the SCP Health Check feature were missing.	3	23.2.2
36377695	NRF Profile is not getting updated with modified NF-setID list from NRF SRV Config	The NRF profile did not get updated with the modified NF-setID list from the NRF SRV Config.	3	23.4.0
36349547	SCP generates 400 bad request with Invalid API version error when the request from consumer is sent with api version as v2	SCP generated a 400 bad request with an invalid API version error when the request from the consumer was sent with API version 2.	3	23.4.0
36349296	SCP routes messages to SEPP irrespective of isInterPLMN flag value in NRF SRV configuration	SCP routed messages to SEPP irrespective of the isInterPLMN parameter value in NRF SRV configuration.	3	23.4.0
36344271	InterSCP metrics are not getting pegged even if SCP-C routes traffic to SCP-P for Model D request with DNS SRV feature enabled.	InterSCP metrics were not getting pegged even when SCP-C routed traffic to SCP-P for Model D requests with the DNS SRV feature enabled.	3	23.4.0

Table 4-53 (Cont.) SCP 24.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36280528	SCP is not able to indicate appropriate cause for number of failed responses received on DNS queries	SCP was unable to indicate the appropriate cause for the number of failed responses received on DNS queries.	3	23.4.0
36262787	SCP is not indicating end point and service ID for ocscp_metric_attempts_to_forward_route_total metric	SCP did not indicate endpoint and service ID for the ocscp_metric_attempts_to_forward_route_total metric.	3	23.4.0
36249830	ocscp_producer_nf_instance_id parameter in the ocscp_metric_nf_lci_tx_total metrics is shown as unknown for all messages related to the performance run	The ocscp_producer_nf_instance_id parameter in the ocscp_metric_nf_lci_tx_total metric was shown as unknown for all messages related to the performance run.	3	23.4.0
36245570	SCP returning undefined error when we edit NF Rule Profile Configuration	SCP returned an undefined error when editing NF Rule Profile Configuration.	3	23.4.0
36210790	SCP : On deleting scp secret from K8 secret scp worker pod went into CrashLoopBackOff state	Upon deleting the SCP secret from the Kubernetes secret, the SCP worker pod entered a CrashLoopBackOff state.	3	23.4.0
36203485	Inconsistency observed in between SCP generates its own OCI and SCP load shows on grafana board	An inconsistency was observed where SCP generated its own Overload Control Information (OCI), but the SCP load did not reflect on the Grafana board.	3	23.4.0
36082479	interPlmnOciEnforcement parameter has no significance in case of local routing & InterSCP OCI config	The interPlmnOciEnforcement parameter had no significance in the case of local routing and InterSCP OCI configuration.	3	23.4.0
36000690	SCP is not triggering SCPProducerOverloadThrottled alert when load reported by LCI header is higher than Onset Threshold value.	SCP did not trigger the SCPProducerOverloadThrottled alert when the load reported by the LCI header was higher than the onset threshold value.	3	23.3.0

Table 4-53 (Cont.) SCP 24.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35842396	CPU Threshold alarms do not match the CPU percentage displayed in the Grafana board metrics.	CPU threshold alarms did not match the CPU percentage displayed in the Grafana board metrics.	3	23.2.2
36731146	Grafana Dashboard KPI Inconsistency	There was an inconsistency in Grafana Dashboard KPIs.	4	23.4.1
36697835	Usage of plmnList to be described in more detail in IG & RG	The usage of plmnList required more detailed description in Oracle Communications Cloud Native Core, Service Communication Proxy Installation, Upgrade, and Fault Recovery Guide and Oracle Communications Cloud Native Core, Service Communication Proxy REST Specification Guide.	4	23.2.2
36562343	SCP is updating the trigger point rule incorrectly when adding header with different values	SCP updated the trigger point rule incorrectly when adding headers with different values.	4	24.1.0

> **Note:**
>
> Resolved bugs from 23.4.3 and 24.1.1 have been forward ported to Release 24.2.0.

4.2.12 SEPP Resolved Bugs

Table 4-54 SEPP 24.2.4 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37586767	SNMP MIB File Issue	The SNMP server was unable to interpret the SNMP traps sent by OCSEPP due to an outdated MIB file. The MIB file has been updated to include the necessary OID and related details.	2	24.2.0

Table 4-54 (Cont.) SEPP 24.2.4 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37521629	"nfApiRoot" shall be updated in SEPP custom yaml to reflect SEPP PLMN IGW details.	The `nfApiRoot` in the `sepp_custom_values_.yaml` file referenced the NRF Ingress Gateway, but it should have been the PLMN Ingress Gateway of SEPP, as this URI is designed to receive notifications from the NRF. The unused parameter has been removed.	3	24.2.0

Table 4-55 SEPP 24.2.3 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37410882	SEPP as a Roaming hub is sending PlmnIdList when it is not supposed to send	When roaming hub was initiating the N32c handshake, it didn't send the PLMN ID list. However, when roaming hub was responding to the N32c handshake request initiated by the Remote SEPP, it was sending the PLMN ID list. This was due to missing check while creating capability-exchange response message in roaming hub mode.	3	23.4.1
37446555	Debug is set to true for app-info in SEPP custom yaml	There was a stale entry in `sepp_custom_values_.yaml`file to set the log level of app-info.	4	24.2.1

Table 4-56 SEPP 24.2.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37356760	SEPP corrupts multipart messages Content-Transfer-Encoding binary.	It was observed that when a multipart message is received at SEPP, the application or vnd.3gpp.5gnas part was being corrupted by the Egress Gateway.	2	24.2.1

Table 4-57 SEPP 24.2.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36677373	Traffic failure on GTW release 24.2.x with IllegalReferenceCount exception on IGW	Continuous traffic failure was observed on Gateway 24.2.x releases with IllegalReferenceCount exception being generated on n32-ingress gateway.	2	24.2.0
37047839	SEPP Call failures with 4xx & 5xx Error codes with 24K MPS traffic with message copy	SEPP call failures were observed with 4xx and 5xx error codes with 24K MPS traffic.	2	24.2.0
36880659	SEPP Ingress Rate Limiting Per RSS not working	In SEPP 23.4.0 release, the Ingress Rate Limiting per RSS was not working. `oc_ingress_rss_ratelimit`metric was getting pegged but the status was displayed as not applied.	3	24.2.0
36897010	SEPP Topology Hiding does not support Multipart message type	Topology hiding feature handler was not able to decode the JSON body within the Multipart Data List Boundary . When a multipart message was received, topology hiding was not getting applied on the message.	3	24.2.0

Table 4-57 (Cont.) SEPP 24.2.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36855523	Message Copy Support At EGW- Query parameter is striped out from path header while copying data to DD	The Query parameter was stripped out from path header while copying data to DD. This issue was observed only on Egress Gateway.	3	24.2.0
36777756	Call failed observed with error code 500,503,504,408 during and n32-ingress-gateway restart with 137-Error code during 56K MPS performance run with Cat3 feature enabled with cache refresh time 120000 at sepp_24.2.0-rc1	During the 56K MPS performance run with Cat-3 feature enabled and cache refresh time 120000 at sepp_24.2.0, n32-ingress-gateway, 137 error code, and and call failure were observed with error code 500, 503, 504,and 408.	3	24.2.0
35925855	x-reroute-attempt-count and x-retry-attempt-count header come twice in response when AR feature is enabled	While running an Alternate routing feature scenario, Duplicate x-reroute-attempt-count and x-retry-attempt-count was being observed in the repsonse. It was observed with both static and dynamic routing.	4	24.2.0

Table 4-58   SEPP 24.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36574528	Request to add workaround for "IllegalReferenceCountException" issue in SEPP Troubleshooting guide	The rectification parameter for `IllegalReferenceCountException` on n32-igw issue must be added in the SEPP Troubleshooting guide. `nettyInboundExceptions: exceptions: - io.netty.util.IllegalReferenceCountException count: 150 // current default is 1000 timePeriod: 1`	3	24.1.0
36453267	Some discrepancy found at SEPP_24.1.0_rc1 default yaml resource profile and sepp 24.1.0 doc resource profile	There were discrepancies in SEPP_24.1.0_rc1 default yaml resource profile and documented resource profile.	3	24.1.0
36388875	RemoteSEPP config parameters are not aligned with REST document	On provisioning Remote SEPP with only the mandatory parameters, the following scenarios were observed: In `Security Edge Protection Proxy User Guide`, `isEnabled` was set to True, but it must be set to False. The domain was configured which was not passed in the POST request.	3	24.1.0

Table 4-58 (Cont.) SEPP 24.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36329085	Helm uninstall is not removing all ConfigMaps impacting automation	When the SEPP was uninstalled, the rate limiting config-maps remained in the namespace. Due to this, subsequent SEPP installation in the same namespace was getting failed.	3	23.3.1
36282658	SEPP 23.3.1 CAT2 Body IE for RURI nausf-auth/v1/ue-authentication has incorect REGEX.	In the Cat -2 feature, the Body IE of RURI nausf-auth/v1/ue-authentication had incorrect REGEX, which does not match standard definition of SUCI.	3	23.3.1
34953499	SEPP-FT-HostedSEPP: HostedSEPP adding two via header in request and response flow.	In HostedSEPP, two via headers were getting added.	3	22.4.0
36282844	SEPP 23.3.1 Global Ingress Rate Limiting Metric and Alerts are not working.	During the initial test of the Global Ingress Rate Limiting feature, it was observed that the feature was working as designed, but the metric *oc_ingressgateway_global_ratelimit_total* was not reporting the drop messages. As a consequence the alerts associated with the feature were not triggered.	3	23.3.1

Table 4-58 (Cont.) SEPP 24.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36616858	SEPP_PERF: call failed with error code 500,503,504,408 observed during 56K MPS performance run with topology Hiding, SCM(Cat0,Cat1,Cat2,Cat3), Overload, Mediation, SOR, RateLimiting feature enabled.	It was observed that approx. 59.62% traffic loss from csepp side and 59.36% traffic loss from psepp side in a 7Hr call run with topology Hiding, SCM(Cat0, Cat1, Cat2, Cat3), Overload, Mediation, SOR, Rate limiting feature enabled at 56K MPS. During the performance run, 56K MPS with topology hiding, SCM(Cat0, Cat1, Cat2, Cat3), Overload, Mediation, SOR, Rate limiting features with cache refresh time 120000ms and 50ms server delay with duration 7Hr. • csepp_call success rate: 59.62% approx. • psepp_call success rate: 59.36% approx. • No restarts were seen. • Perfgo deployed on hardhead1 cluster with 10server & 09client each side. • Run with with 50ms server delay • Feature Enabled:- topology Hiding, SCM(Cat0, Cat1, Cat2, Cat3), Overload,	3	24.1.0

Table 4-58 (Cont.) SEPP 24.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
		Mediation, SOR, RateLimiting feature enabled at SEPP_24.1.0-GA.		

34627763	SCP-SEPP_FT: pn32f_jetty, cn32f_jetty, pn32f_server_latency and cn32f_server_latency metrics are not being pegged	The following metrics were not being logged:
		`ocsepp_pn32f_jetty_request_stat_metrics`
		`ocsepp_cn32f_jetty_request_stat_metrics`
		`ocsepp_pn32f_server_latency`
		`ocsepp_cn32f_server_latency`
			3	22.3.0

36653115	content-type header being sent from SEPP to UDR while fetching auth status	Removed the `content-type` parameter content type from cat-3 GET API call.	3	22.4.0
34374452	Residue pending in DB after deleting 900 RS created	On scaling down pn32c and cn32c pods if a delete request was run for Remote SEPP, 204 was returned but the entry was not deleted. Also, no error was displayed when the POST request was executed when the pods were scaled down.	3	22.2.0
35907257	On a fresh installed SEPP setup errors observed in appinfo pod.	On a fresh installed SEPP setup, errors were observed in the appinfo pod.	3	23.3.0
36393100	Multiple responses for metric ocsepp_cn32c_handshake_reInitiation_req_total	In the metric `ocsepp_cn32c_handshake_reInitiation_req_total` , the order of the peer_plmn_id was different in the two responses.	4	24.1.0

Table 4-58 (Cont.) SEPP 24.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36368414	Creating RemoteSeppSet is allowed with only secondary or tertiary SEPP	Primary, Secondary, and Tertiary parameters were marked as mandatory in documents, but they should be marked as conditional.	4	23.4.0
36322466	For alert SEPPConfigMgrRouteFailureAlert incomplete summary is displayed	The summary was incomplete for `SEPPConfigMgrRouteFailureAlert`.	4	23.4.0
36202185	SEPP 23.2.1 CAT2 header passed for non provisoned PLMN ID	In the Cat -2 feature, the handling of PLMN IDs had to be revised to segregate different PLMN. Example 262 025 and 262 02.	4	23.2.1
35912471	For mediation default error title should be configured	In the CNC Console GUI, navigate to SEPP and go to Mediation, the Mediation Feature and Error Configuration details are available on the screen. The error title must be present by default.	4	23.3.0
36252767	Egress Gateway is not adding authority information to DD for TXrequests	It was observed that HTTP URI authority information was not included in the transmitted information to DD for TXRequests for NRF and SEPP by the Egress Gateway.	4	23.4.0

Table 4-58 (Cont.) SEPP 24.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36622258	SEPP - Missing egress flows to alert manager in network policies	The Egress flows to prometheus, the appinfo/perf-info needs access to alertmanager. This was not yet covered by the 24.1.0 network policies of SEPP.	4	24.1.0
36710549	Message copy SSL feature paramenters not present	The Message copy feature SSL parameters were not present in the `Security Edge Protection Proxy Installation, Upgrade, and Fault Recovery Guide`.	4	23.2.1
36649460	SEPP User Guide Architecture Diagram has incorrect representations for flows and environment	It was observed that the architecture diagram must be updated in the `Security Edge Protection Proxy User Guide` 24.1.0, as there are some incorrect call flows. It was also noted that there may be a need for a separate diagram for the OCI environment.	4	24.1.0
36577733	oc_ingressgateway_incoming_tls_connections metric counter coming in -ve	In some scenarios, `oc_ingressgateway_incoming_tls_connections` metrics count was displayed as -1 on Prometheus which was incorrect. The metrics count should always be a positive number.	4	24.1.0

Table 4-58 (Cont.) SEPP 24.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36553303	Correct dimensions for ocsepp_pn32f_latency metrics in user guide	The peer_plmn_id dimension was not displayed for metrics `ocsepp_pn32f_latency_seconds_count` and `ocsepp_pn32f_latency_seconds_sum` but was documented in the *Security Edge Protection Proxy User Guide*. For the metric `ocsepp_pn32f_latency_seconds_max`, the dimension nfInstanceId must be updated to nf_instance_id. The dimensions peer_plmn_id and targetUrl were not displayed.	4	24.1.0
36510421	SEPP-PERF: PN32F minimum value shown in negative on Grafana.	PN32F minimum value was shown in negative on Grafana. *{peer_fqdn="sepp2.inter.oracle.com", remote_sepp_name="sepp1"}**Min:-52.3s Max: 24.5s Avg:4.63s**Formula:- *sum(irate(ocsepp_pn32f_latency_seconds_sum{namespace=~"$Namespace"}[2m])) by(peer_fqdn,remote_sepp_name) / sum(irate(ocsepp_pn32f_latency_seconds_count\{namespace=~"$Namespace"}[2m])) by(peer_fqdn,remote_sepp_name)	4	24.1.0

Note:

Resolved bugs from 24.1.0 have been forward ported to Release 24.2.0.

4.2.13 UDR Resolved Bugs

Table 4-59 UDR 24.2.5 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37963997	Unexpected restart of cnUDR pods	cnUDR pods were restarting unexpectedly.	2	24.2.4
37910137	cnUDR 24.2.0 doesn’t reply to UDR Diameter messages, but it does reply to SNR messages	cnUDR 24.2.0 was not replying to UDR diameter messages but was replying to Subscribe Notification Request (SNR) messages.	3	24.2.0
37785011	DIAMGW POD restart observed while running peformance for 10K SH & 17.2K N36 for 24 Hours with DB restart	Diameter gateway pod was restarting when running performance test for 10K and 17.2K N36 for 24 hour duration with database restart.	3	25.1.100
37984384	PNRs Sent to Old Peers When Multiple SUBSCRIPTION Entries Exist for Same Subscriber	Push Notification Request (PNR) was sent to old peers when multiple subscription entries exist for the same subscriber.	3	24.2.0

Table 4-60 UDR 24.2.4 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37776149	PNR isn't sent if SNR and Change in the user profile are done through different cnUDRs	PNR (Push Notification Request) was not sent if the Subscribe Notification Request (SNR) and user profile were updated through two different cnUDR.	2	24.2.0

Table 4-60 (Cont.) UDR 24.2.4 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37660632	PNR is not generated for Sh interface when diamproxy fqdn is changed	Push Notification Request (PNR) was not generated for diameter SH when diameter proxy Fully Qualified Domain Name (FQDN) was changed.	3	24.2.0
37511228	UDR is sending Multiple Resources under "delResources" parameter in notification of subscriber deletion	UDR was sending multiple resources under `delResources` parameter in the notification of subscriber deletion.	3	24.2.0

Table 4-61 UDR 24.2.3 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37388443	Bulk Import Tool importing custom parameters with "\" character	There was an extra backslash ("\") in the JSON structure of custom parameters for the Bulk Import Tool.	2	24.2.0
37467819	Pod protection feature doesn't include Memory as resource	Memory as resource was included in the Pod Protection feature.	3	24.2.0
37301547	Subscriber Export Tool Status in the GUI does not update during export	The CNC Console did not update the Subscriber Export Tool status.	3	24.2.0

Table 4-62 UDR 24.2.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36790601	SLF- After microservice restart overload discard were not happening still after hitting L4 alerts	When microservice was restarted, overload discard was not happening after L4 alerts.	3	24.2.0

Table 4-63   UDR 24.2.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36813453	During Performance for Call Model 1- 25K SH Traffic drops to 15K SH.	The diameter SH traffic was dropping from 25K to 15K during Performance Call Model for 25K diameter SH traffic.	3	24.2.0

> **Note:**
>
> Resolved bugs from 24.1.x have been forward ported to Release 24.2.1.

Table 4-64   UDR 24.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36398645	UDR is sending Multiple Resources in notification for Subscriber deletion during Active Gx session	When the subscribers were deleted during the active GX session, UDR was sending multiple resources in notification to Policy Control Function (PCF).	3	24.1.0
36424133	Unable to import the 4G policy data exml export file into cnUDR after ixml conversion with multiple msisdn keys	Unable to import the 4G policy data EXML export file into cnUDR after IXML was converted with multiple Mobile Station Integrated Services Digital Network (MSISDN) keys.	3	24.1.0
36605832	SLF-Shared CNDB yaml resources are mismatching with the benchmarking guide of 24.1.0	There was a mismatch in the resources between CNDB yaml file and UDR Benchmarking Guide.	3	24.1.0
36605566	"ndb_allow_copying_alter_table" should be ON in SLF provided CNDB 24.1.0 yaml	The `ndb_allow_copying_alter_table` parameter was set as OFF in the CNDB yaml file.	3	24.1.0

Table 4-64 (Cont.) UDR 24.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36398329	404 failure message is missing for POST request in subscriber trace	During POST update request in the subscriber trace, 404 failure message was missing.	4	24.1.0

Note:

Resolved bugs from 24.1.x have been forward ported to Release 24.2.0.

4.2.14 Common Services Resolved Bugs

4.2.14.1 ATS Resolved Bugs

ATS 24.2.0 Resolved Bugs

There are no resolved bugs in this release.

4.2.14.2 ASM Configuration Resolved Bugs

Release 24.2.0

There are no resolved bugs in this release.

4.2.14.3 Alternate Route Service Resolved Bugs

Table 4-65 Alternate Route Service 24.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36761736	igw-cache, egw-cache and altsvc-cache shall change the Port "notused"to "http2-notused"	Each Egress Gateway pod had around 394 incoming connections. It was observed that Egress Gateway traffic was not treated as HTTP2 traffic rather than TCP proxy.	2	23.2.7
36730520	Typo in alternate-route service account label section	There was a typo in service account label section of alternate route service charts.	3	24.1.0

Note:

Resolved bugs from 24.1.x have been forward ported to Release 24.2.0.

4.2.14.4 Egress Gateway Resolved Bugs

Table 4-66 Egress Gateway 24.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36617874	SM PCF egress traffic failing after 23.4.2 Upgrade	NRF Client sent an empty data frame in addition to the GET request while sending a GET request towards Egress Gateway.	1	23.4.3
36682966	EgressGW http2.remote_reset	"http2.remote_reset" was observed in Egress Gateway logs.	2	23.2.12
36761736	[igw-cache, egw-cache and altsvc-cache shall change the Port "notused"to "http2-notused"	Each Egress Gateway pod had around 394 incoming connections. When checked, It was found that Egress Gateway traffic was not treated as HTTP2 traffic rather TCP proxy.	2	23.2.7
36574019	Traffic failures when SBI Routing is enabled at EGW	When SBI routing was enabled at Egress Gateway, there was high latency, and traffic failure was observed at Egress Gateway.	2	24.1.5
35750433	Incorrect deletion of action set and criteria set	A check on the deletion of the action set and criteria set was required when routesconfiguration was configured.	3	23.3.3
36357662	With Invalid Via header and with HTTPS request failure response is coming	NSSF should not have sent an error response if AMF has sent an invalid Via header in the nsselection request. It should have sent the success response without the LCI and OCI headers.	3	23.4.0
36522768	All egress gateway replica pods are pegging the available peers metric, resulting in the value of the metric more than the actual available peers count	When all Egress Gateway replica pods were pegged to the available peers metric, the value of the metric was higher than the actual available peers count.	3	24.1.5

Note:

Resolved bugs from 24.1.x have been forward ported to Release 24.2.0.

4.2.14.5 Ingress Gateway Resolved Bugs

Table 4-67   Ingress Gateway 24.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
36761736	igw-cache, egw-cache and altsvc-cache shall change the Port "notused"to "http2-notused"	Each Egress Gateway pod had around 394 incoming connections. It was found that Egress Gateway traffic was not treated as HTTP2 traffic rather TCP proxy.	2	23.2.7
35527387	DNS SRV Support-Loss of SEPP forwarding Traffic at IGW with DNS SRV enabled at high TPS	When SEPP forwarding traffic was run at the rate of 2100 TPS,it was observed that the latency at n32-igw suddenly increased. This impacted the overall latency of SEPP performance. There were no errors observed in the n32-igw logs.	2	23.2.3
36472065	ProvGW Ingress Gateway TLS scenarios are failing with NullPointerException	TLS requests to Provgw for 23.2.0 version, which had Ingress Gateway 23.2.4, started failing suddenly with NullPointerException (100% failures).	2	23.2.0
36684616	Post upgrade to 23.4.3, Policy Create, Policy Update and Policy Delete have error 403 Forbidden	After upgrading to PCF 23.4.3, Ingress Gateway experienced 403 errors (SM CREATE / UPDATE / DELETE).	2	23.2.12

Table 4-67 (Cont.) Ingress Gateway 24.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
36594692	IGW should support the its own NF Instance ID for aud field in Oauth Access token	Ingress Gateway should have supported its NF Instance ID for aud field in the Oauth Access token.	2	24.1.6
35661396	IGW is not doing case-insensitive check while validating CCA header	All extension names, path parameters, and instance IDs were not compared or validated to check the case-insensitivity while performing CCA header validation.	3	23.2.4
36289424	If User-Agent Header is invalid, (HTTPS enabled) should not add the LCI and OCI Header	When AMF sent an invalid User-Agent header in a nsselection request, NSSF should not have included the LCI or OCI headers in the response because the peer information was invalid.	3	23.4.0
36337091	After updating values via HELM upgrade , discards occurring with previous config in Global Ingress Rate Limiting	After updating values through the Helm upgrade, discards occurred with the previous configuration in Global Ingress Rate Limiting.	3	23.3.2
35490934	Prometheus: alternate-route service being down causes altsvc-cache service down alarms	When the alternate-route service pod was down, altsvc-cache metrics were indicatedas down because there was no IP exposed in Kubernetes.	3	22.4.5

Table 4-67 (Cont.) Ingress Gateway 24.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
36312914	Incorrect 3gpp-sbi-origination-timestamp sent from PCF to BSF which gets originated from IGW	When PCF sent the extra orig-3gpp-sbi-origination-timestamp in the BSF binding request, 3gpp-sbi-origination-timestamp should have carried the same values from the N7 Create, but it did not. Instead, orig-3gpp-sbi-origination-timestamp held the timestamp of the N7 timestamps.	3	23.2.6
36388781	Pod protection rest configuration is not updated in database	The pod protection rest configuration was not updated in the database.	3	24.1.2

Note:

Resolved bugs from 24.1.x have been forward ported to Release 24.2.0.

4.2.14.6 Common Configuration Service Resolved Bugs

Table 4-68 Common Configuration Service 24.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36539330	IGW configurations are reset on reinstall when DB contains data	NRF common configuration data was reset to default when installed with a database backup.	2	24.1.5

Note:

Resolved bugs from 24.1.x have been forward ported to Release 24.2.0.

4.2.14.7 Helm Test Resolved Bugs

Table 4-69 Helm Test 24.2.0 Known Bugs

Bug Number	Title	Description	Severity	Found in Release
35101768	Helm Test should avoid Hook PODs from its list while doing Health Check	Helm test should avoid Hook pods from its list while doing health check.	3	23.1.0
36683862	ERROR logs are getting printed on Successful execution of HELM TEST	The Helm test was successful, but error logs were printed in the pod logs.	3	24.2.0

4.2.14.8 App-Info Resolved Bugs

Release 24.2.0

There are no resolved bugs in this release.

4.2.14.9 NRF-Client Resolved Bugs

Table 4-70 NRF-Client 24.2.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36798428	Discovery cache feature - discovery_cache_support_cache_non_cache_total metric is being exploded	When Discovery cache feature was enabled and the `supi` parameter was part of the query params in the discovery cache, the `discovery_cache_support_cache_non_cache_total` exploded.	4	23.4.3

4.2.14.10 Perf-Info Resolved Bugs

Release 24.2.0

There are no resolved bugs in this release.

4.2.14.11 Debug Tool Resolved Bugs

Release 24.2.0

There are no resolved bugs in this release.

4.3 Known Bug List

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

4.3.1 BSF Known Bugs

BSF 24.2.3 Known Bugs
There are no known bugs in this release.

Table 4-71 BSF 24.2.2 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37033987	nrf-client POD in CrashLoopBackOff after GRR	When the caching feature is utilized by nf-discovery pod, BSF does not have any use for nf-discovery.	When the caching feature is utilized by nf-discovery pod, BSF does not have any use for nf-discovery. **Workaround**: Recover the Nrf-client to manually create the ocbsf_nrf_client DB again on the restored site. The user can run the same command that is used during the installation to create the DB. For an example, for single site, multi site steps can be used accordingly when needed: `CREATE DATABASE IF NOT EXISTS ocbsf_nrf_client CHARACTER SET utf8; GRANT SELECT, INSERT, UPDATE, DELETE, CREATE, DROP, REFERENCES,`	2	23.4.2

Table 4-71 (Cont.) BSF 24.2.2 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
			`INDEX,ALTER ON ocbsf_nrf_client.* TO 'bsfprivilegedusr'@'%';`		

Table 4-72 BSF 24.2.1 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37128193	Make the (BSF) GW header compression backward compatible	Before 24.1.0, the behaviour of BSF to compress/hpack/index the HTTP2 headers was by default. In 24.1.0, this behaviour was incorrectly changed to not compress the pseudo header ":method".	All the HTTP/2 headers are not compressed in absence of HTTP2 headers configuration to compress/hpack/index. **Workaround**: Set the appropriate configuration in the custom-values.yaml file by providing the following list of headers, which do not require indexing: `headerIndexing: doNotIndex:`	3	24.2.0

Table 4-73 BSF 24.2.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36715017	No health request going out from egress GW to SCPas expected from MOP	There are no health requests going out from Egress Gateway to SCP.	Egress Gateway was not able to create and maintain an SCP Health Table, which is used for selecting eligible SCP for routing. **Workaround**: Remove the `httpConfiguration` from `peerSetConfiguration` and restart all the Egress Gateway pods.	3	23.2.4
36912417	BSF Management error handling feature is failing due to a missing validation when loading up new configurations	BSF_Error_Response_Enhancements feature fails as Error handling flag is disabled from BSF Management logs	Overwriting the error response handling configuration with bulk import could not change the required configuration. **Workaround**: Change the required configuration through CNC Console and avoid bulk import for error response handling configuration.	3	24.2.0

Table 4-73 (Cont.) BSF 24.2.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36912994	BSF Diam-gw throwing DOC warning when congestion is not enabled	BSF Diameter Gateway shows DOC warning when congestion is not enabled.	There is no functional impact. The warning logs along with the metrics for congestion gives a false impression that the system is under stress even when the traffic rate is well within bounds. **Workaround**: There is no workaround available.	3	24.2.0

4.3.2 CNC Console Known Bugs

CNC Console 24.2.4

There are no known bugs in this release.

CNC Console 24.2.3

CNC Console 24.2.3 is a Critical Patch Update. Critical Patch Updates provide security patches for supported Oracle on-premises products. They are available to customers with valid support contracts. For more information, see Critical Patch Updates, Security Alerts and Bulletins.

CNC Console 24.2.2

There are no known bugs in this release.

CNC Console 24.2.1

There are no known bugs in this release.

CNC Console 24.2.0

There are no known bugs in this release.

4.3.3 cnDBTier Known Bugs

Table 4-74 cnDBTier 24.2.5 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37842445	`dbtreplmgr` script is unable to stop the replica on HTTPS and TLS-enabled setup on cnDBTier	`dbtreplmgr` script is unable to stop the replica on HTTPS and TLS-enabled setup.	`dbtreplmgr` script cannot be used when HTTPS is enabled to start and stop replication. **Workaround**: Perform the steps given in the *Starting or Stopping cnDBTier* section in *Oracle Communications Cloud Native Core, cnDBTier User Guide* to start and stop replication.	3	24.2.5

Table 4-75 cnDBTier 24.2.4 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37622137	DR getting stuck for non-fatal scenario on prefix enabled 3-channel setup	Georeplication recovery freezes when pod and container prefix is enabled. This behaviour is observed in a three-channel replication setup when georeplication recovery is initiated for non-fatal scenarios.	The DB replication service may get stuck at the `ShutdownSql` stage during georeplication recovery, when the worker node is slow in scheduling a new thread. **Workaround**: Edit the leader `db-replication-svc` deployment and set the value of `"DR_STATE_WAIT_COUNT_AFTER_SHUTDOWN_SQL"` to *"120s"*.	3	25.1.100
37761092	GRR is getting stuck at the `RECONNECTSQLNODES` state	Georeplication recovery is getting stuck at the `RECONNECTSQLNODES` state. This behaviour is observed on a two-site, three-channel replication setup, when DB replication service is performed for a non-fatal error case.	The Georeplication recovery may get stuck at `RECONNECTSQLNODES` state, when DB replication service is performed for a non-fatal error case. **Workaround**: Restart the `db-replication-svc` pod.	3	24.2.0

Table 4-76 cnDBTier 24.2.3 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36487409	dbtpasswd doesn't retain the old password in some of the pods	The `dbtpasswd` script doesn't retain the old password for some of the pods.	While using the `dbtpasswd` script, application pods with old password may not be able to connect to cnDBTier database. The connection of application pods depends on the mysqld pod that is used to attempt the connection with cnDBTier database. If the mysqld pod is one of the affected pods, then the connection fails. **Workaround:** Restart the application pods with the old passwords, so that the pods get the new password from Kubernetes secret.	3	23.4.2

cnDBTier Release 24.2.2

There are no new known bugs in this release. For the existing known bugs, see "cnDBTier 24.2.1 Known Bugs".

cnDBTier Release 24.2.1

Table 4-77 cnDBTier 24.2.1 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36665039	Replication Went Down during NEF DBTier Upgrade from v23.4.3 to 24.2.0-rc.1	Georeplication fails in NEF during a cnDBTier upgrade from 23.4.3 to 24.2.0.	NEF georeplication fails with remote cnDBTier clusters. This requires you to perform georeplication recovery procedures to restore the georeplication with remote cnDBTier clusters. **Workaround:** Divert the NEF traffic from the current cnDBTier cluster to other remote cnDBTier clusters and then perform the upgrade of the current cnDBTier cluster. Repeat the same approach to upgrade other remote cnDBTier clusters.	3	24.2.1

Table 4-77 (Cont.) cnDBTier 24.2.1 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36487409	dbtpasswd doesn't retain the old password in some of the pods	The dbtpasswd script doesn't retain the old password in some of the pods.	While using the dbtpasswd script, application pods with old password may not be able to connect to cnDBTier database. The connection of application pods depends on the mysqld pod that is used to attempt the connection with cnDBTier database. If the mysqld pod is one of the affected pods, then the connection fails. **Workaround:** Restart the application pods with the old passwords, so that the pods get the new password from Kubernetes secret.	3	23.4.2

cnDBTier Release 24.2.0

Table 4-78 cnDBTier 24.2.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36795445	CNDBTier ndbappmysqld and db monitor service pods restarts observed with Exit Code 137	Increased memory usage of ndbappmysqld pods during long runs leads to restarts of the ndbappmysqld pods.	Restart of ndbappmysqld pods lead to pod outage which affects the NF access to database and NF traffic. **Workaround:** • This issue will be resolved in cnDBTier release 24.2.1. Therefore, refrain from installing cnDBTier 24.2.0 and install the revised cnDBTier version (24.2.1) when available. • cnDBTier doesn't support upgrade from 24.2.0 to 24.2.1.	2	24.2.0

Table 4-78   (Cont.) cnDBTier 24.2.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36665039	Replication Went Down during DBTier Upgrade from v23.4.3 to 24.2.0-rc.1	Georeplication fails during an upgrade from 23.4.3 to 24.2.0.	Georeplication fails with remote cnDBTier clusters. This requires you to perform georeplication recovery procedures to restore the georeplication with remote cnDBTier clusters. **Workaround:** Divert the traffic from the current cnDBTier cluster to other remote cnDBTier clusters and then perform the upgrade of the current cnDBTier cluster. Repeat the same approach to upgrade other remote cnDBTier clusters.	3	24.2.0
36487409	dbtpasswd doesn't retain the old password in some of the pods	The `dbtpasswd` script doesn't retain the old password in some of the pods.	While using the `dbtpasswd` script, application pods with old password may not be able to connect to cnDBTier database. The connection of application pods depends on the mysqld pod that is used to attempt the connection with cnDBTier database. If the mysqld pod is one of the affected pods, then the connection fails. **Workaround:** Restart the application pods with the old passwords, so that the pods get the new password from Kubernetes secret.	3	23.4.2

4.3.4 CNE Known Bugs

Table 4-79 CNE 24.2.6 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36740199	BareMetal CNE installation on X9-2 servers fails	When X9-2 server boots with Oracle Linux 9.x (OL9.x) Unbreakable Enterprise Kernel (UEK) ISO, the screen runs for a while, and then stalls with the an error message *Device doesn't have valid ME Interface*.	BareMetal CNE cannot be installed on X9-2 servers. **Workaround:** Use x8-2 servers or use CNE 23.3.x or older on X9-2 servers.	2	23.4.1
36818112	CNLB Metrics pipeline does not work after cnlb app pods logs start throwing errors	CNLB metrics report problems when high volume of data is returned. This occurs specially when cnlb app has been running for long duration.	CNLB metrics will not work, but CNLB app will continue to work. **Workaround:** Disable CNLB metrics.	2	24.2.0
36843512	The Cnlb app pods fails to configure network when network names do not end with numeric values on `cnlb.ini` file	When CNLB app tries to configure IPs from sig on sig2 and sig3 network interfaces, configuration fails and pod then restarts. This is due to the network names provided as "sig, sig2, sig3".	CNLB app causes network issues and pod restarts. **Workaround:** Name the sig network interfaces as "sig0", if there are multiple networks with subtsring as "sig" and no numeric value.	3	24.2.0

CNE 24.2.4 Known Bugs

There are no new known bugs in this release. For existing known bugs, see "CNE 24.2.1 Known Bugs".

CNE 24.2.3 Known Bugs

There are no new known bugs in this release. For existing known bugs, see "CNE 24.2.1 Known Bugs".

CNE 24.2.2 Known Bugs

There are no new known bugs in this release. For existing known bugs, see "CNE 24.2.1 Known Bugs".

Table 4-80 CNE 24.2.1 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36740199	bmCNE installation on X9-2 servers fail	Preboot execution environment (PXE) booting occurs when installing Oracle Linux 9 (OL9) based BareMetal CNE on X9-2 servers. The OL9.x ISO UEK kernel installation hangs on X9-2 server. When booted with OL9.x UEK ISO, the screen runs for a while and then hangs with the following message "Device doesn't have valid ME Interface".	BareMetal CNE installation on X9-2 servers fails. **Workaround**: Perform one of the following workarounds: • Use x8-2 servers. • Use CNE 23.3.x or older version on X9-2 servers.	2	23.4.1

Table 4-80 (Cont.) CNE 24.2.1 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36818112	CNLB Metrics pipeline stops to work after cnlb app pods logs starts throwing errors	CNLB metrics encounter issues when high volume of data is returned. This happens specially when CNLB application runs for a long time.	CNLB metrics doesn't work, however CNLB application continues to work. **Workaround:** Disable CNLB metrics.	2	24.2.0
36874451	OCCNE lb-controller pods stops processing service events or producing logs	The `lb-controller` pod is stuck and does not function after displaying the following exception in the logs. This exception is seen intermittently. `FileNotFoundError: [Errno 2] No such file or directory: '/etc/exabgp/log'`	`lb-controller` pod hangs and doesn't function. **Workaround**: Restart the `lb-controller` pod.	3	24.1.0
36843512	Cnlb app pods fails to configure network when network names do not end with numeric values on cnlb.ini file	CNLB application pods fail to configure network, when network names are provided in the following patterns: `"sig, sig2, sig3"`. CNLB application tries to configure IPs from `sig` on `sig2` and `sig3` network interfaces causing issues and restarts.	CNLB application causes network issues and pod restarts. **Workaround**: Name `sig` network interfaces as `"sig0"`, if you have multiple networks with subtsring as `"sig"` and no numeric value.	3	24.2.0

Table 4-81 CNE 24.2.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36740199	bmCNE installation on X9-2 servers fail	Preboot execution environment (PXE) booting occurs when installing Oracle Linux 9 (OL9) based BareMetal CNE on X9-2 servers. The OL9.x ISO UEK kernel installation hangs on X9-2 server. When booted with OL9.x UEK ISO, the screen runs for a while and then hangs with the following message "Device doesn't have valid ME Interface".	BareMetal CNE installation on X9-2 servers fails. **Workaround**: Perform one of the following workarounds: • Use x8-2 servers. • Use CNE 23.3.x or older version on X9-2 servers.	2	23.4.1
36818112	CNLB Metrics pipeline stops to work after cnlb app pods logs starts throwing errors	CNLB metrics encounter issues when high volume of data is returned. This happens specially when CNLB application runs for a long time.	CNLB metrics doesn't work, however CNLB application continues to work. **Workaround:** Disable CNLB metrics.	2	24.2.0

Table 4-81 (Cont.) CNE 24.2.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36843512	Cnlb app pods fails to configure network when network names do not end with numeric values on cnlb.ini file	CNLB application pods fail to configure network, when network names are provided in the following patterns: `"sig, sig2, sig3"`. CNLB application tries to configure IPs from `sig` on `sig2` and `sig3` network interfaces causing issues and restarts.	CNLB application causes network issues and pod restarts. **Workaround**: Name `sig` network interfaces as `"sig0"`, if you have multiple networks with subtsring as `"sig"` and no numeric value.	3	24.2.0

OSO 24.2.5

There are no known bugs in this release.

OSO 24.2.0

There are no known bugs in this release.

4.3.5 NEF Known Bugs

NEF 24.2.0 Known Bugs

There are no known bugs in this release.

4.3.6 NRF Known Bugs

NRF 24.2.4 Known Bugs

Table 4-82 NRF 24.2.4 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37412089	For NFSetId case-sensitive validation, registration request is getting accepted for NID having value not compliant to fixed length of 8 digit hexadecimal number as per 3GPP	For NFSetId case-sensitive validation, the `NFRegister` or `NFDiscover` service operations request is accepted for non-compliant Network Identifier (NID) values. As per 3GPP, NID value did not have a fixed length of 8 digit hexadecimal number.	NRF accepts the `NFRegister` or `NFDiscover` service operations request with non-compliant NID value. **Workaround**: NFs should use a fixed length of 8 digit hexadecimal number for NID value as per 3GPP for `NFRegister` or `NFDiscover` service operations request.	3	23.4.6

Table 4-82   (Cont.) NRF 24.2.4 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37760595	Discovery query results in incorrect match with preferred-locality=US%2bEast	NRF is returning NFProfile ordered at first position with locality matching with *space* (for example, US East) while query contains *plus* as special character (for example, US+East).	In NFProfile in response from NRF, locality with *space* is placed first and then followed by the localities with the special character. **Workaround**: Locality attribute must not have *space* or *plus* as special characters. If query has %252B as encoded character, then NFProfile with *plus* sign will match, for example, US+East.	3	24.2.4

Table 4-82   (Cont.) NRF 24.2.4 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37784967	DiscoveryResultLoadThreshold feature, discovery response contains Profile having load value(30) greater then DiscoveryResultLoadThreshold (20)	For the discoveryResultLoadThreshold feature, NFProfile is returned in the NFDiscover response without checking the load at the NFProfile level under the following conditions: • service-names query parameter is present in NFDiscover service operation query. • Filtered NFProfile has only one NFService. • load is not present at NFservice level.	This scenario is only applicable in case of discoveryResultLoadThreshold feature, when service-names query parameter is present in NFDiscover service operation query and filtered NFProfile has only one NFService and that NFService doesn't have load. **Workaround**: Disable the feature by setting the `discoveryResultLoadThreshold` parameter value as **0**.	3	24.2.4

Table 4-82 (Cont.) NRF 24.2.4 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37788289	Discovery query results in Empty Profile when discovery query is forwarded due to AMF profile is Suspended and Empty response received from Forwarded NRF	When discovery query is received with Globally Unique AMF Identifier (GUAMI) query parameters for AMF target NF type and the matching profiles are in SUSPENDED state, it is expected that the SUSPENDED profiles are returned in the discovery response when emptylist feature is enabled. However, the SUSPENDED profiles are not returned.	Consumer NFs will not receive SUSPENDED profiles when the Consumer NFs try to discover AMF with GUAMI. **Workaround**: None. If forwarding is enabled, then it is possible that the response will contain SUSPENDED profiles from the other segment.	3	24.2.4
37412138	Error response generated by NRF needs to be corrected when registration request is sent with incorrect order for mcc and mnc	Error response generated by NRF should be corrected when registration request is sent with incorrect order for Mobile Country Code (mcc) and Mobile Network Code (mnc).	There is no impact on signaling message processing. The error message details don't include correct error reason. **Workaround**: There is no workaround available.	4	23.4.6

Table 4-82 (Cont.) NRF 24.2.4 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37797310	NFRegistration logs some attributes are showing wrong data	Some attributes in the NFRegistration logs has incorrect data.	Some attributes in the NFRegistration logs has incorrect data. **Workaround**: There is no workaround available.	4	24.2.4

NRF 24.2.3 Known Bugs

NRF 24.2.3 is a Critical Patch Update. Critical Patch Updates provide security patches for supported Oracle on-premises products. They are available to customers with valid support contracts.

For more information, see Critical Patch Updates, Security Alerts, and Bulletins.

Table 4-83 NRF 24.2.3 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37412089	For NFSetId case-sensitive validation, registration request is getting accepted for NID having value not compliant to fixed length of 8 digit hexadecimal number as per 3GPP	For NFSetId case-sensitive validation, the `NFRegister` or `NFDiscover` service operations request is accepted for non-compliant Network Identifier (NID) values. As per 3GPP, NID value is compliant to a fixed length of 8 digit hexadecimal number.	NRF will accept the `NFRegister` or `NFDiscover` service operations request with non-compliant NFSetID containing NID digits. **Workaround**: NFs should use correct length of NID digits as per 3GPP for NFRegister or NFDiscover service operations request.	3	23.4.6

Table 4-83 (Cont.) NRF 24.2.3 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37412138	Error response generated by NRF needs to be corrected when registration request is sent with incorrect order for mcc and mnc	Error response generated by NRF should be corrected when registration request is sent with incorrect order for mcc and mnc.	There is no impact on signaling message processing. The error message details don't include correct error reason. **Workaround**: There is no workaround available.	4	23.4.6

NRF 24.2.2 Known Bugs

There are no known bugs in this release.

Table 4-84 NRF 24.2.1 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36792455	NRF-ndbappmysqld pods restarts observed with Exit Code 137 and db-monitor pod restarts with given resource profile	Traffic failure is seen due to ndbappmysqld pod restart due to memory issues.	During the periodic restarts of ndbappmysqld pods, which occur approximately every 17 hours, very low traffic failure may occur. This is mitigated by the fact that over 99% of read operations, constituting the majority of total traffic, retrieve data from the in-memory cache. **Workaround**: Increasing memory of ndbappmysqld pods can delay the restart of the pods.	2	24.2.0
36856077	CNCC Edit and Delete Operations both not working together in edit screen	CNC Console Edit and Delete operations were not working together on the edit screen.	On CNC Console GUI, Edit and Delete operations will not work together on single edit screen. **Workaround**: Cancel the ongoing edit by clicking Cancel and edit again. Use only one operation at a time. Either edit or delete the row.	3	24.2.0

NRF 24.2.0 Known Bugs

Table 4-85 NRF 24.2.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36792455	NRF-ndbappmysqld pods restarts observed with Exit Code 137 and db-monitor pod restarts with given resource profile	Traffic failure is seen due to ndbappmysqld pod restart due to memory issues.	During the periodic restarts of ndbappmysqld pods, which occur approximately every 17 hours, very low traffic failure may occur. This is mitigated by the fact that over 99% of read operations, constituting the majority of total traffic, retrieve data from the in-memory cache. **Workaround**: Increasing memory of ndbappmysqld pods can delay the restart of the pods.	2	24.2.0

Table 4-85 (Cont.) NRF 24.2.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36856077	CNCC Edit and Delete Operations both not working together in edit screen	CNC Console Edit and Delete operations were not working together on the edit screen.	On CNC Console GUI, Edit and Delete operations will not work together on single edit screen. **Workaround**: Cancel the ongoing edit by clicking **Cancel** and edit again. Use only one operation at a time,either edit or delete the row.	3	24.2.0

4.3.7 NSSF Known Bugs

Release 24.2.1

Table 4-86 NSSF 24.2.1 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37136539	[dnsSrvEnabled: false] [peer Health monitoring: disabled] NSSF is not sending the notification towards peer2 host if peer1 is down	When DnsServices is disabled and static routes are used, the notifications are not getting rerouted in scenario where primary peer is SCP is down.	Loss of notification message in a specific corner case when static routine is being used **Workaround:** Enable dnsSrv and use virtual FQDNs.	3	24.2.1

Table 4-86 (Cont.) NSSF 24.2.1 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37136248	If dnsSrvEnabled is set to false and peer1 is used as a virtual host, the egress gateway will not sending the notifcation to peer2 host and peer health status is empty	When DnsServices is disabled and virtual host is used for peer 1 and static routes is used for peer2, the notifications are not getting rerouted in scenario where primary peer health status is empty.	Loss of notification message in a specific corner case when static routine is being used Workaround Enable dnsSrv and use virtual FQDNs.	3	24.2.1

Release 24.2.0

Table 4-87 NSSF 24.2.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36817882	Auth & Rule table updated for Tailist and Tairange list for the slice which is restricted in Tai during NSAVailability update procedure for white list AMF but in response same is not coming.	An issue during the upgrade from version 24.1.0 to 24.2.0 causes Ingress Gateway to lose OAuth certificates.	Due to the lost certificates, the OAuth configuration is effectively wiped out after the upgrade. This can lead to disruptions in services until a new access token is obtained and the certificates are reconfigured. **Workaround**: After upgrading to version 24.2.0, manually reconfigure the OAuth validator configuration.	3	24.2.0
36817980	NSSF is sending Tacrangelist in response for NSAvailability procedure but not created in DB (Auth & Rule table) for NSAvailability procedure.	NSSF is sending a *Tacrangelist* in the nsavailability response, but the corresponding entry is not created in the database for the *Tacrangelist* {"start":"003000","end":"004000"}, resulting in a discrepancy between the response and the database state.	There is no impact on traffic as it is a configuration issue. **Workaround**: No workaround available	3	24.2.0

Table 4-87 (Cont.) NSSF 24.2.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36823225	Wrong error response title and DB (Auth & rule table) not cleared during the subs-mod replace operation for White listed AMF.	In nsavailability PUT procedure and subsequent subscription modification replace operation, the response contains a wrong string, and the entry is not cleared from the database. This issue also occurs when the slice is TA (tracking area)restricted.	There is no impact on traffic as it is a configuration issue. **Workaround**: No workaround available	3	24.2.0
36823604	2-site GR setup ASM Enabled: Failover with overload : 15K TPS: while traffic reached to 15K(150% traffic), NSSF has dropped 13.9 percentage traffic with 500 error code and latency of ns-selection is 573 ms.	In a 2-site GR setup with ASM enabled, during a failover with overload at 15K TPS, NSSF drops 13.9% of traffic with a 500 error code and a latency of 573 ms in nsselection.	There is no impact on traffic as it is a configuration issue. **Workaround**: No workaround available	3	24.2.0
36838710	Multiple unsubscription happening while the initial unsubscription request sends 204 response	Unsubscription is happening multiple times, even when the initial unsubscription succeeds, causing unnecessary messages in the network.	There is no impact on traffic as it is a configuration issue. **Workaround**: No workaround available	3	24.2.0
36838930	Oauth Configuration had vanished on its own after we upgrade the NSSF {24.1.0 to 24.2.0-rc.2}	The OAuth configuration vanishes on its own after upgrading NSSF.	There is no impact on traffic as it is a configuration issue. **Workaround**: No workaround available	3	24.2.0

Table 4-87 (Cont.) NSSF 24.2.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36844482	[Alternate-route cache is not deleting the SCP entry after TTL(Time to live)	The Alternate-route cache does not delete the SCP entry after the TTL (time to live) expires, resulting in the cache still containing the entry and returning a 200 response instead of a 404 during a deregister request.	There is no impact on traffic as it is a configuration issue. **Workaround**: No workaround available	3	24.2.0
36678392	NSSF-CNCC Server header configuration done with wrong NF type while User agent header have proper validation for NF type	In the REST-based configuration API, invalid configurations are being accepted. In such instances, additional validations are required.	There is no impact on traffic as it is a configuration issue. **Workaround**: No workaround available	3	24.1.0
36668249	NSSF-CNCC Get response of config param "NSSF Backup" have param "nssfSystemOptionDtoList" which is not as per REST Docs	The response of "NSSF Backup" API includes parameter "*nssfSystemOptionDtoList*," which is not specified in the NSSF REST API Guide.	There is no impact on traffic as it is a configuration issue. **Workaround**: No workaround available	3	24.1.0

Table 4-87 (Cont.) NSSF 24.2.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36667357	NSSF-CNCC "NSSF System Option" validation check is not present while configuring via CNCC	Validation checks on mandatory parameters were not performed during the configuration of System Options. Configuration should not succeed without providing mandatory fields.	There is no impact on traffic as it is a configuration issue. **Workaround**: Validation check has been added to all the mandatory parameters and corresponding junits. ATS test cases have been added for various scenarios.	3	24.1.0
36662095	NSSF-CNCC Ingress GW Configuration param level as "Warning" missing from list for Overload control discard policy configuration	NSSF - CNC Console Ingress Gateway configuration parameter level "Warning" is missing from the drop-down list of options for Overload Control Discard Policy configuration.	There is no impact on traffic as it is a configuration issue. **Workaround**: Warning needs to added in the list of policy configuration in the GW services.	3	24.1.0

Table 4-87 (Cont.) NSSF 24.2.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36662054	NSSF-CNCC Ingress pod Discard Policy mapping configured without mandatory param	Discard Policy mapping is configured without mandatory parameters.	There is no impact on traffic as it is a configuration issue. **Workaround**: Policy name and service name should be made mandatory parameter in the UI field.	3	24.1.0
36653435	NSSF is not validating the Algo while validating the access token in non-asm setup.	NSSF is not validating the algorithm while validating the access token in a non-ASM setup.	There is no impact on traffic. **Workaround**: Operator is suggested to use ES256 algorithm in both Oauthvalidator and in access token.	3	24.1.0
36653405	Signature should validate for access token in non-asm setup	Signature is not validating the access token in a non-ASM setup.	There is no impact on traffic. **Workaround**: Access token needs to be signature verified using (CA Authority) NRF certificate and public key.	3	24.1.0

Table 4-87 (Cont.) NSSF 24.2.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36640866	NSSF-CNCC CNCC UI Stuck sometime while trying to do various configuration	CNC Console UI sometimes gets stuck while trying to perform various configurations or switching screens to edit different objects.	There is no impact on traffic as it is a configuration issue. **Workaround**: No workaround available	3	24.1.0
36635475	NSSF-CNCC Egress GW SBI Error Criteria set not configured when status series and status configured in response	For Egress Gateway config, SBI Error Criteria is not being set when the status series and status are configured in response.	There is no impact on traffic as it is a configuration issue. **Workaround**: Corresponding documentation changes are required.	3	24.1.0
36633989	NSSF-CNCC User agent header configured without mandatory param	TUser-Agent header is configured without providing mandatory param "*nfInstanceId*". This is a validation issue.	There is no impact on traffic as it is a configuration issue. **Workaround**: NfInstance ID should be made a mandatory parameter.	3	24.1.0

Table 4-87 (Cont.) NSSF 24.2.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36625525	NSSF-CNCC - Server header configuration done successfully without mandatory param	Server header configuration succeeds without the mandatory parameter.	There is no impact on traffic as it is a configuration issue. **Workaround**: Nftype should have validations for right configuration.	3	24.1.0
36573848	Deregister request towards alternate-route is not working	Deregister requests are giving 404 error code.	There is no impact on traffic. **Workaround**: No workaround available	3	24.1.0
36552026	KeyId, certName, kSecretName, and certAlgorithm invalid values are not validating in the oauthvalidator configuration.	KeyId, certName, kSecretName, and certAlgorithm are displaying invalid values resulting in failure of validation for the oauthvalidator configuration.	There is no impact on traffic. **Workaround**: While configuring oauthvalidator, operator needs to use the correct values.	3	24.1.0

Table 4-87 (Cont.) NSSF 24.2.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36528105	3.5K TPS 99.99% Failures seen when Rate-limiting feature is enabled in ASM setup	For 10K traffic run, the user is facing 50% traffic loss when ratelimiting feature is enabled.	50% loss on traffic is observed. **Workaround**: Correct configurations for 10K traffic need to be calculated when rateLimiting is enabled.	3	24.1.0
36285762	After restarting the NSselection pod, NSSF is transmitting an inaccurate NF Level value to ZERO percentage.	Intermittently, NSSF displays 0% NF percent load during a restart scenario, but NF service load is not zero. The condition corrects itself within a few minutes after the pod starts.	There is no impact on traffic. **Workaround**: No workaround available	3	23.4.0
36265745	NSSF is only sending NF-Instanse/NF-Service load level information for multiple AMF Get Requests	Only in one setup, NSSF is intermittently sending only Instance Load despite NF service level load being calculated.	There is no impact on traffic. **Workaround**: No workaround available	3	23.4.0

Table 4-87 (Cont.) NSSF 24.2.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36168261	NSSF does not discard packets as per the level configuration in ocdiscard policies.	NSSF is not discarding the exact amount of traffic as configured in discard policies when the error rate exceeds the threshold. When NSSF reaches a critical level based on the error rate instead of rejecting 50%, the observed reject rate is 33.2%.	There is minimal impact on traffic. The reduction in discard percentage is observed only when the traffic contains more than 20% of error. Also, there is no impact on CPU as when the traffic is run for longer time, the CPU percentage is not increasing. **Workaround**: This is how the backend algorithm at Ingress Gateway works. It takes average of previous discarded traffic in the sampling period, resulting in actual discarded traffic not being same as configured discard	3	23.4.0

Table 4-87 (Cont.) NSSF 24.2.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
			percentage.		
36158880	[Server Header] Patch operation is not working for errorcodeserieslist, Routeconfig & serverheaderdetails with NSSF 23.4.0	Patch operation to update certain parameters for *errorcodeserieslist*, routes config, and server header details API sometimes malfunctions.	There is minimal to no impact on traffic. **Workaround**: When Patch operation fails, PUT operation can be used to complete the configuration.	3	23.4.0
35975971	"User agent header support" NSSF is not adding User agent header in Registration, patch, Discovery & subscription towards NRF when "overwriteHeader :false " & in notification msg	NSSF is not adding User-Agent header despite the feature being enabled when the Overwrite header is set to false towards NRF.	There is no impact on traffic. **Workaround**: Set Overwrite header as true.	3	23.3.0

Table 4-87 (Cont.) NSSF 24.2.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35971708	while pod protection is disabled, OcnssfIngressGatewayPodResourceStateMajor alert is not clear and resource metric is not updating to -1	NSSF is not clearing alerts when Pod Protection feature is disabled.	There is no direct impact on traffic. Once pod protection feature is disabled NSSF does not look at the state of gateway pod, which leads to not clearing the metrics. **Workaround**: Refer to the resource state in Prometheus.	3	23.3.0
35962306	In a congested state, NSSF should reject a new incoming HTTP2 connection when AcceptIncomingConnections is set to false - Randomly Behaviour	NSSF is intermittently accepting connection when in the congested state. The connection request should be rejected in this scenario.	There is a chance of restart if this behavior continues. However, as per the testing, this is intermittent. **Workaround**: No workaround available	3	23.3.0

Table 4-87 (Cont.) NSSF 24.2.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35922130	Key Validation is missing for IGW pod protection parameter name configuration	Ingress Gateway REST API configuration has missing validations for Pod Protection feature.	There is no impact on traffic. **Workaround**: Configure NSSF with correct values as per the REST API Guide.	3	23.3.0
35921656	NSSF should validate the integer pod protection parameter limit.	The Rest API for configuration of pod protection has missing validations for the parameter *Limit*.	No impact. **Workaround**: Operator should configure the values as per the NSSF REST API guide.	3	23.3.0
35888411	Wrong peer health status is coming "DNS SRV Based Selection of SCP in NSSF"	NSSF is not showing unhealthy status for a nonexistent SCP. In case peerConfiguration is done with the first peer as nonexistent SCP and the second peer as virtual Host, the peerHealth status is wrongly shown with peer1 as healthy, although it is nonexistent.	There is no impact on traffic as non-responsive SCP is not being considered for status. **Workaround**: No workaround available	3	23.3.0
35860137	In Policy Mapping Configuration in Ingress Gateway, For the samplingPeriod parameter, max value of parameter validation should be necessary.	The Rest API for configuration of *ocpolicymapping* has missing validations.	There is no impact on traffic. **Workaround**: Operator can configure the values as per the NSSF REST API guide.	3	23.3.0

Table 4-87 (Cont.) NSSF 24.2.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35502848	Out of Range Values are being configured in PeerMonitoringConfiguration (Support for SCP Health API using HTTP2 OPTIONS)	REST API for configuration of *ocpolicymapping* and *PeerMonitoringConfiguration* has missing validations.	There is no impact on traffic. **Workaround**: Operator can configure the values as per the NSSF REST API guide.	3	23.2.0
36297806	NSSF is only sending NF-Instanse/NF-Service load level information for multiple AMF Get Requests	When multiple AMFs send requests to nsselection microservice, for some requests, either NF-Instance scope LCI headers or NF-Service scope LCI headers are returned.	There is no impact on traffic. **Workaround**: No workaround available	3	23.4.0
36298095	After restarting the NSselection pod, NSSF is transmitting an inaccurate NF Level value to ZERO percentage.	After restarting the nsselection pod, NSSF is transmitting an inaccurate NF Level value.	There is no impact on traffic. **Workaround**: The operator must configure Rule and Map with a Network Slice profile rather than a default PLMN profile.	3	23.4.0

Table 4-87 (Cont.) NSSF 24.2.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36634002	NSSF-CNCC Peer monitoring configuration done successfully with provided Values "out of range"	Peer monitoring configuration is done successfully with provided Values "out of range". Configuration should happen within the provided range.	There is no impact on traffic. **Workaround**: Operator can configure the values within the range as per the NSSF REST API guide.	3	24.1.0
36653053	NSSF-CNCC Get key need to be removed from CNCC UI for "NSSF Restore" configuration since get functionality is not being supported for respective config param	*Get* button should be removed from CNC Console UI for "NSSF Restore" configuration as get functionality is not supported for respective config parameter.	There is no impact on traffic. **Workaround**: No workaround available	3	24.1.0
35986361	NSSF will not modify the weight values in metrics simultaneously if the weight value changes. The weight metric has changed when any pod raises a new alarm.	NSSF as part of pod protection raises alerts when POD is in DOC condition. Once an alert is raised and the condition is updated, the alert does not get cleared.	There is no impact on traffic. **Workaround**: No workaround available	4	23.3.0
35855937	In Ingress Gateway's Error Code Series Configuration, The names of the exceptionList and errorCodeSeries parameters are not verified.	REST API for configuration of *errorcodeserieslist* has missing validations.	There is no impact on traffic. **Workaround**: Operator can configure the values as per the NSSF REST API guide.	4	23.3.0

Table 4-87 (Cont.) NSSF 24.2.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35855745	Missing validation of the failureReqCountErrorCodeSeriesId mandatory parameter in the Ingress Gateway's Routes Configuration.	REST API for configuration of *routesconfiguration* has missing validations.	There is no impact on traffic. **Workaround**: Operator can configure the values as per the NSSF REST API guide.	4	23.3.0
35855377	The abatementValue less than onsetValue should be validated by NSSF in the Overload Level Threshold Configuration.	REST API for configuration of Overload Level Threshold has missing validations. Abatement value greater than onset value is configured in OverloadThreshold configuration, which is not correct.	There is no impact on traffic. **Workaround**: Operator can configure the values as per the NSSF REST API guide.	4	23.3.0
35796052	In Service Solution upgrade ASM enabled2 Site GR Setup, Latency increases (237ms on site2 and 228ms on site2) observed during in service solution NSSF upgrade both sites from NSSF version 23.2.0 to 23.3.0	Intermittently, during in-service upgrade validation, the latency exceeds the threshold of 50ms and reaches up to 237ms for some messages.	There is no impact on traffic or service as this does not cause a timeout. **Workaround**: No workaround available	4	23.3.0
35297857	If AMF and NSSF enabled ONSSAI feature, NSSF should reject the ns-availability subscriptions request when taiList IE is non-empty array in ns-availability subscriptions request.	NSSF supports both the *taiList* and *taiRangeList*; however, there is a discrepancy in the specification as both cannot be supported together. As the support exists for both parameters separately, this issue is being maintained until further clarity is obtained from the specifications.	There is no impact on traffic. **Workaround**: No workaround available	4	23.1.0

4.3.8 OCCM Known Bugs

OCCM 24.2.3 Known Bugs

OCCM 24.2.3 is a Critical Patch Update. Critical Patch Updates provide security patches for supported Oracle on-premises products. They are available to customers with valid support contracts. For more information, see Critical Patch Updates, Security Alerts and Bulletins.

OCCM 24.2.2 Known Bugs

OCCM 24.2.2 is a Critical Patch Update. Critical Patch Updates provide security patches for supported Oracle on-premises products. They are available to customers with valid support contracts. For more information, see Critical Patch Updates, Security Alerts and Bulletins.

OCCM 24.2.1 Known Bugs

There are no known bugs in this release.

OCCM 24.2.0 Known Bugs

There are no known bugs in this release.

4.3.9 OCI Adaptor Known Bugs

OCI Adaptor 24.2.1 Known Bugs

There are no known bugs in this release.

OCI Adaptor 24.2.0 Known Bugs

There are no known bugs in this release.

4.3.10 Policy Known Bugs

Policy 24.2.6 Known Bugs

There are no known bugs in this release.

Policy 24.2.5 Known Bugs

There are no known bugs in this release.

Table 4-88 Policy 24.2.4 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37611224	Few parameters are missing from REST API GET request	A few parameters are missing from REST API GET request.	There is no customer impact. **Workaround**: There is no workaround available.	3	24.2.4

Policy 24.2.3 Known Bugs

There are no known bugs in this release.

Policy 24.2.2 Known Bugs

There are no known bugs in this release.

Table 4-89   Policy 24.2.1 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release

37127652	Make the GW header compression backward compatible.	Before 24.1, the behaviour of PCF to compress/ hpack/index the HTTP2 headers was by default. In 24.1.0, this behaviour was incorrectly changed to not compress the pseudo header ":method".	All the HTTP/2 headers are not compressed in absence of HTTP2 headers configuration to compress/hpack/index.
			Workaround:
			Set the appropriate configuration in the custom-values.yaml file by providing the following list of headers, which do not require indexing:
			`headerIndexing:`
			`doNotIndex:`
				3	24.3.0

Table 4-89 (Cont.) Policy 24.2.1 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36727061	36727061	The remote variables for both projects got created correctly after Gx CCR-I. But, after the Gx CCR-U processing, PCRF-Core project specific variables were not updated on the UDR and only UM project SSVs were getting updated.	When both PCRF-Core and UM have remote SSVs created or updated in the respective policy projects, they are created correctly on Gx CCR-I. But, after Gx CCR-U processing, PCRF-Core project specific variables are not updated on the UDR. Only the UM policy project related SSVs are updated. **Workaround**: The UM Policy and PCRF Core policies needs to segregate their variables which can be done by configuration. This would enable the algorithm to correctly merge the SSVs (received in the UM Decision and PCRF PRE decision) and subsequently send all variables to PDS for external update (PATCH) to UDR.	3	23.4.2
36942043	In case UDR responds with ERROR 503 for subs-to-notify, PCF-UDR-connector update failure metric "ocpm_udr_tracking_response_total" twice	In case UDR responds with ERROR 503 for subs-to-notify, PCF-UDR-connector updates the failure metric "ocpm_udr_tracking_response_total" twice.	In case of a specific error scenario mentioned in the bug, "ocpm_udr_tracking_response_total" metrics is getting pegged twice. There is no signaling or end user impact. **Workaround**: There is no workaround available.	4	24.2.0

Table 4-89 (Cont.) Policy 24.2.1 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36928821	Usage-monitoing pod logs are not included in the Subscriber activity log	Usage monitoiring logs in a usage monitoring policy are not included in the Subscriber Activity log when enabled. This makes diffcult to troubleshoot one particular IMSI as there is no logs from that service.	Usage-mon subscriber activity log works for all the messages except "CREATE". **Workaround**: There is no workaround available.	4	24.4.3

Table 4-90 Policy 24.2.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36832070	Issue with "Enforcement Network Element Name" blockly	"Enforcement Network Element Name" blockly is causing the Policy Rule Engine (PRE) to halt its evaluation of the Policy tree when encountered.	Though there is no signaling failure, some of the sessions are responded with success without any charging rule. **Workaround**: There is no workaround available.	2	23.2.8
36601868	PCRF 23.2.8 - Performance is significantly impacted when the database has many records	The performance is impacted when traffic is migrated due to the high quantity of records.	It may impact the performance at high TPS, above ~18K TPS for a specific call model. There is no functional impact. **Workaround**: There is no workaround available.	2	23.2.8

Table 4-90 (Cont.) Policy 24.2.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36884531	PCRF performance run observed Binding serv error "Invalid compressed data" & "No content to map due to end-of-input\n at [Source: (String)\"\";	Performance issues with data call due to Binding service errors when data compression scheme is enabled.	When data compression scheme is enabled for binding service, deregistration fails with ""Invalid compressed data" & "No content to map due to end-of-input\n at [Source: (String)\"\" error. Deregistration succeeds if data compression scheme is disabled. **Workaround**: Update the binding service DB_URL deployment variable and remove "characterSetResults=UTF-8&".	2	24.2.0
36915221	[AM_UE Performance] upgrade fails from PCF 24.1.0_GA to 24.2.0_rc7 " Error creating bean with name 'hookService' defined in URL"	Upgrade from any of the previous releases to Policy 24.2.0 fails due to Helm upgrade failure during post-upgrade job for nrf-client-nfdiscovery. This is due to an exception in deleting the older release entry from common_configuration table for `nrf-client-nfdiscovery` service.	This upgrade failure causes traffic loss. **Workaround**: In case the upgrade from any of the previous releases to Policy 24.2.0 fails, retry the upgrade, which will delete the older version's configuration enabling upgrade to go through. If the retry fails, manually delete the older version entries from common_configuration table and retry the upgrade. This can bring up the services with newer version's configuration data.	3	24.2.0
36909037	PRE performance degradation when using MatchList in Policy Table	PRE shows degradation in performance when a matchlist functionality is used in the Policy Table. This leads to latency issues with PRE.	PRE was showing degradation in performance when a matchlist functionality was used with the Policy Table. **Workaround**: There is no workaround available.	3	24.2.0

Table 4-90   (Cont.) Policy 24.2.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36913031	pcrf-core calls latency increases in seconds when bulwark locking mechanism is integrated with the Gx interface	Latency of PCRF Core calls increase in seconds when locking mechanism using Bulwark service is integrated with the Gx interface.	Latency of PCRF Core calls increases by seconds when locking mechanism with Bulwark service is used. **Workaround**: There is no workaround available.	3	24.2.0
36740591	PCF is not retrying PATCH with Updated ETAG if UDR respond with 412 Pre-Condition Failed	PCF is not retrying PATCH with Updated ETAG if UDR responds with 412 Pre-Condition Failed. PCRF is expected to retry PATCH Request with latest ETAG Value	There can be data loss in case of terminate request as the PATCH can fail with 412 error code. Usage Monitoring service can trigger a DELETE request, which will delete the usage-monitoring record from PDS database. This issue has no impact in the case of an UPDATE request. **Workaround**: There is no workaround available.	3	24.2.0

4.3.11 SCP Known Bugs

Release 24.2.4

SCP 24.2.4 is a Critical Patch Update. Critical Patch Updates provide security patches for supported Oracle on-premises products. They are available to customers with valid support contracts.

For more information, see Critical Patch Updates, Security Alerts, and Bulletins.

There are no known bugs in this release.

Release 24.2.3

SCP 24.2.3 is a Critical Patch Update. Critical Patch Updates provide security patches for supported Oracle on-premises products. They are available to customers with valid support contracts.

For more information, see Critical Patch Updates, Security Alerts, and Bulletins.

Known bug from 24.2.0 has been forward ported to Release 24.2.3.

SCP 24.2.2 Known Bugs

Known bug from 24.2.0 has been forward ported to Release 24.2.2.

SCP 24.2.1 Known Bugs

Known bug from 24.2.0 has been forward ported to Release 24.2.1.

Table 4-91   SCP 24.2.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release

36698507	TLS Handshake fails intermittently with TLS version 1.3 after idle timeout	The Transport Layer Security (TLS) handshake intermittently fails with TLS version 1.3 after idle timeout.	TLS connections would fail to reestablish intermittently but were successful on the next attempt.
			Workaround:
			Enabling the pre-shared key extension resolved the issue.
			Update the `ocscp_values.yaml` file by uncommenting `clientDisabledExtensions` and `serverDisabledExtensions`, and then redeploy SCP.
			The following snippet from the `ocscp_values.yaml` file displays the uncommented parameters:
			`enableTlsExtensionsCompliance: true`
			`#uncomment clientDisabledExtensions and serverDisabledExtensions in case`
				3	24.2.0

Table 4-91 (Cont.) SCP 24.2.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
			golang version is lower than latest of 1.18 clientDisabledExtensions: session_ticket,status_request,status_request_v2,psk_key_exchange_modes,early_data,certificate_authorities serverDisabledExtensions: session_ticket,status_request,status_request_v2,psk_key_exchange_modes,early_data,certificate_authorities		

4.3.12 SEPP Known Bugs

SEPP 24.2.4

There are no known bugs in this release.

SEPP 24.2.3

There are no known bugs in this release.

SEPP 24.2.2

There are no known bugs in this release.

SEPP 24.2.1

There are no known bugs in this release.

Table 4-92 SEPP 24.2.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
36677373	Traffic failure on Gateway release 24.2.x with IllegalReferenceCount exception on Ingress Gateway.	There is continuous traffic failure with Gateway 24.2.x releases and IllegalReferenceCount exception is getting generated on n32-ingress gateway. The issue is visible once the traffic hits 2500 TPS per gateway pod.	his scenario is leading to a consistent traffic drop of 2 to 3 percent. **Workaround**: Run at a reduced capacity of 24K MPS. A potential fix is available from the GW team and is currently being validated. The fix will be delivered in the next patch.	2	- GW 24.2.1 - GW 24.2.0
36767431	Call failed observed with error code 500,503,504,408 during and n32-ingress-gateway restart with 137-Error code during 56K MPS performance run with Cat3 feature enabled with cache refresh time 120000 at sepp_24.2.0-rc1	There is a continuous traffic failure with the Gateway 24.2.x releases and IllegalReferenceCount exception when Cat-3 feature is enabled.	This scenario is leading to a consistent traffic drop of 2 to 3 percent. **Workaround**: Run at a reduced capacity of 24K MPS. A potential fix is available from the GW team and is currently being validated. The fix will be delivered in the next patch.	2	24.2.0

Table 4-92 (Cont.) SEPP 24.2.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
35898970	DNS SRV Support- The time taken for cache update is not same TTL value defined in SRV record.	The time to update the cache is not the same as the TTL defined in SRV records. Sometimes the cache updates even before TTL expires and in other instances, the cache updates later than the TTL. The expectation is that the cache must update as per TTL, i.e. once TTL is expired, hence if TTL is 60, then the cache must update after every 60s.	If the priority or weight is changed, it might take a longer time than TTL to get the cache updated and reflect the changes in the environment. **Workaround**: After changing the configuration, restart the n32-egress-gateway and alternate-route-svc.	3	23.4.0
36777756	Call failed observed with error code 500,503,504,408 during 56K MPS performance run with SOR feature enabled at sepp_24.2.0-rc1	There is a continuous traffic failure with the Gateway 24.2.x releases and are the IllegalReferenceCount exception when SOR feature is enabled.	This scenario is leading to a consistent traffic drop of 2 to 3 percent. **Workaround**: Run at a reduced capacity of 24K MPS.A potential fix is available from the GW team and is currently being validated. The fix will be delivered in the next patch.	3	24.2.0

Table 4-92 (Cont.) SEPP 24.2.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
36616858	Call failed with error code 500, 503,504, 408 observed during 56K MPS performance run with topology Hiding, SCM(Cat0, Cat1, Cat2, Cat3), Overload, Mediation, SOR, RateLimiting feature enabled.	There is a continuous traffic failure with the Gateway 24.2.x release and are the IllegalReferenceCount exception when security features are enabled.	This scenario is leading to a consistent traffic drop of 2 to 3 percent. **Workaround**: Run at a reduced capacity of 24K MPS.A potential fix is available from the GW team and is currently being validated. The fix will be delivered in the next patch.	3	24.1.0
35919133	DNS SRV Support- Custom values key "dnsSrvEnabled" does not function as decsribed	Custom values key dnsSrvEnabled description mentions the use of #Flag to control if DNS-SRV queries are sent to core DNS or not. If the flag is true, the request should go to coreDNS. If the flag is false, it must not go to coreDNS. Even when the flag is made false and the setup is upgraded, the curl reaches core DNS. Scenario: When the flag is made false and peerconfig is created for the virtual FQDN, the expectation was that on executing curl, it must not be able to resolve the virtual FQDN since the flag is false, hence the request must not reach core DNS.	In the case of virtual FQDN, the query will always go to core DNS. **Workaround**: Do not configure records in core DNS.	3	23.4.0

Table 4-92 (Cont.) SEPP 24.2.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
36263009	PerfInfo calculating ambiguous values for CPU usage when multiple services mapped to single pod	In the `cgroup.json` file, multiple services are mapped to a single endpoint. The calculation of CPU usage is ambiguous. This impacts the the overall load calculation	The overall load calculation is not correct. **Workaround**: No workaround available.	3	23.4.1
36672456	WARNING level displayed as BLANK on Discard Policy CNCC Screen	When the user navigates to the Overload Discard Policies screen, 4 levels (Warning, Major, Minor, and Critical) are configured but while displaying the level name, "Warning" is not displayed and is blank while other levels are not.	The user will not be able to set a warning level. **Workaround**: No workaround available.	3	24.2.0
36672487	No error thrown while enabling Discard Policy Mapping to true when corresponding discard policy is deleted	No error is thrown while enabling Discard Policy Mapping to true when the corresponding discard policy is deleted. Steps to reproduce: 1. Delete discard policy "Policy2" in overload discard policies of n32 igw. 2. Enable discard policy in Discard Policy Mapping to true with Policy name as "Policy2". Configuration is saved successfully but it should throw an error as Discard Policy "Policy2" is deleted.	If the user enables discard policy mapping to true and the discard policy does not exist, the error will not be visible. **Workaround**: Helm configuration can be used to configure overload discard policies.	3	24.2.0

Table 4-92 (Cont.) SEPP 24.2.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
36419802	For Error responses, no message is copied on DD from IGW & EGW when message copy is enabled	When a request is sent to EGW or IGW, and EGW or IGW sends an error code (503,408,500, etc) for the request, neither the request nor the response is copied to DD.	There is no customer impact. **Workaround**: No workaround available.	3	24.1.2
36605744	Generic error is thrown when wrong configuration is saved via GW REST APIs	Generic error is thrown (Could not validate Json) when the wrong configuration is saved via GW REST API's/CNC Console Screen. Error reason should be specific to which mandatory parameter is missing.	It is a generic error that makes it difficult for the user to troubleshoot the issue. **Workaround**: There is no workaround available.	3	24.2.0
36614527	[SEPP-APIGW] Overload Control discard policies not working with REST API and CNCC	The user is not able to edit or change the Overload Control discard policies default values. It is showing the error "ocpolicymapping doe snot contain this policy name" on saving the configuration. The same behavior is observed with REST API.	The user will not be able to edit overload discard policies through CNC Console. **Workaround**: Helm configuration can be used to configure overload discard policies.	3	24.2.0
35925855	x-reroute-attempt-count and x-retry-attempt-count header come twice in response when AR feature is enabled	Duplicate x-reroute-attempt-count and x-retry-attempt-count are observed.	There is no customer impact. There are duplicate headers. **Workaround**: No workaround available.	4	23.3.0

Table 4-92 (Cont.) SEPP 24.2.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
36577846	Improper value of InstanceIdentifier in oc_egressgateway_outgoing_tls_connections metric	Incorrect value of InstanceIdentifier in the oc_egressgateway_outgoing_tls_connections metric.	None. The InstanceIdentifier value is not correct in tls-connection metrics, but metrics can be uniquely identified on the basis of namespace. **Workaround**: No workaround available.	4	24.2.0
36666519	Producer/ Consumer FQDN contain ":port" while messageCopy is enabled on GWs	For the header 3gpp sbi api root '3gpp-sbi-target-apiroot': 'http://RJBAR.UDCVMH.HSS02.UDM.5gc.mnc011.mcc724.3gppnetwork.org:8080'} The FQDN(both producer and consumer) should not contain port as per 3GPP specs. Observation: 'producer-fqdn': 'RJBAR.UDCVMH.HSS02.UDM.5gc.mnc011.mcc724.3gppnetwork.org:8080', Expected: 'producer-fqdn': 'RJBAR.UDCVMH.HSS02.UDM.5gc.mnc011.mcc724.3gppnetwork.org',	There is no customer impact. **Workaround**: No workaround available.	4	23.4.0

Table 4-92 (Cont.) SEPP 24.2.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
36605719	Warnings being displayed while installing mediation due to k8sResource.container.prefix/suffix parameter	The warning is as follows: *helm install -f custom.yaml ocsepp ocsepp/ -nns* *coalesce.go:286: warning: cannot overwrite table with non table for ocsepp.k8sResource.container.prefix (map[])* *coalesce.go:286: warning: cannot overwrite table with non table for ocsepp.k8sResource.container.suffix (map[])* *coalesce.go:286: warning: cannot overwrite table with non table for ocsepp.nf-mediation.global.k8sResource.container.prefix (map[])* *coalesce.go:286: warning: cannot overwrite table with non table for ocsepp.nf-mediation.global.k8sResource.container.suffix (map[])* The above warnings are displayed due to the parameters suffix and prefix present in mediation charts with the value "{}". The installation will be successful but warnings should not be displayed.	There is no customer impact. Extra warnings are visible in the Helm install. **Workaround**: No workaround available.	4	24.1.0

4.3.13 UDR Known Bugs

UDR 24.2.5 Known Bugs

There are no new known bugs in this release. Known bugs from 24.2.4 have been forward ported to release 24.2.5.

UDR 24.2.4 Known Bugs

Table 4-93 UDR 24.2.4 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36094811	Migration tool performance issue to read records from 4G UDR at high TPS	There is performance issue while the Migration Tool is reading records from 4G UDR at high Transactions per second (TPS).	The duration of data migration has increased. **Workaround**: There is no workaround available.	3	23.4.0
36381825	Helm chart does not pass Helm Strict Linting	Helm chart is not passing Helm strict linting.	There is no impact. **Workaround**: The duplicate errors from Helm strict lint must be ignored.	3	22.3.2
36810163	Sender value in the Notify-service error log should be same as server header value sent by Egressgateway	The value in the notify-service error log must be same as the server header value sent by the Egress Gateway.	This only affects the logging. The server header is not used by notify server for application logic. **Workaround**: There is no workaround available.	3	24.2.0

UDR 24.2.3 Known Bugs

There are no new known bugs in this release. Known bugs from 24.2.0 have been forward ported to release 24.2.3.

UDR 24.2.2 Known Bugs

There are no new known bugs in this release. Known bugs from 24.2.0 have been forward ported to release 24.2.2.

UDR 24.2.1 Known Bugs

There are no new known bugs in this release. Known bugs from 24.2.0 have been forward ported to release 24.2.1.

UDR 24.2.0 Known Bugs

Table 4-94 UDR 24.2.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36094811	Migration tool performance issue to read records from 4G UDR at high TPS	There is performance issue while the Migration Tool is reading records from 4G UDR at high Transactions per second (TPS).	The duration of data migration has increased. **Workaround**: There is no workaround available.	3	23.4.0
36381825	Helm chart does not pass Helm Strict Linting	Helm chart is not passing Helm strict linting.	There is no impact. **Workaround**: The duplicate errors from Helm strict lint must be ignored.	3	22.3.2
36810163	Sender value in the Notify-service error log should be same as server header value sent by Egressgateway	The value in the notify-service error log must be same as the server header value sent by the Egress Gateway.	This only affects the logging. The server header is not used by notify server for application logic. **Workaround**: There is no workaround available.	3	24.2.0
36829216	UDR is sending Multiple Resources under "delResources" parameter in notification of subscriber deletion	UDR sends multiple resources with `delResources` parameter in the notification of subscriber deletion.	This only affects subscriber deletion and does not affect the deletion og individual resources. **Workaround**: There is no workaround available.	3	24.2.0

4.3.14 Common Services Known Bugs

4.3.14.1 ATS Known Bugs

ATS 24.2.0 Known Bugs

There are no known bugs in this release.

4.3.14.2 ASM Configuration Known Bugs

Release 24.2.0

There are no known bugs in this release.

4.3.14.3 Alternate Route Service Known Bugs

Alternate Route Service 24.2.0 Known Bugs

There are no known bugs in this release.

4.3.14.4 Egress Gateway Known Bugs

Table 4-95 Egress Gateway 24.2.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35948415	The PUT API allows you to add cause values to the "sbiroutingerrorcriteriasets" in policy 23.2.2.	The PUT API allows you to add cause values to "`sbiroutingerrorcriteriasets`" in Policy 23.2.2. The following parameters are introduced in the Error cause-based re-try feature in the 23.2.6 patch and 23.4.0 releases, however, configuration details can be added in the previous releases, such as 23.2.2 and 23.2.4:`"cause":{"path":".cause","reason":["UNSPECIFIED_MSG_FAILURE","SUBSCRIPTION_NOT_FOUND"`.	Non applicable configuration is being allowed with PUT API operation. **Workaround**: There is no workaround available.	3	23.2.2

Table 4-95 (Cont.) Egress Gateway 24.2.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36730017	Register request towards alternate-route is giving incorrect response of 200	While performing the register request, Egress Gateway received 200 OK response, however, the FQDN entry is absent in DNS Server.	There is no customer impact. **Workaround**: There is no workaround available.	4	24.1.0

4.3.14.5 Ingress Gateway Known Bugs

Table 4-96 Ingress Gateway 24.2.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36677373	Traffic failure on GTW release 24.2.x with IllegalReferenceCount exception	Observed continuous traffic failure with GTW 24.2.x, and the IllegalReferenceCount exception is generated on n32-ingress gateway.	Complete traffic loss is observed during high performance run beyond certain limit. **Workaround**: There is no workaround available.	2	24.2.1

Table 4-96 (Cont.) Ingress Gateway 24.2.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36672487	No error thrown while enabling Discard Policy Mapping to true when corresponding discard policy is deleted	No error is thrown while enabling Discard Policy Mapping to true when the corresponding discard policy is deleted Steps to reproduce:- 1. Delete discard policy "Policy2" in Overload discard policies of n32 igw 2. Enable discard policy in Discard Policy Mapping to true having Policy name as "Policy2" Configuration is saved successfully but it should throw an error as Discard Policy "Policy2" is deleted	If the user enabled discard policy mapping to true and the discard policy does not exist, the error will not be visible. **Workaround**: Helm configuration can be used to configure overload discard policies.	3	24.2.0
35983677	NRF- Missing mandatory "iat claim" parameter validation is not happening in CCA header for feature - CCA Header Validation	Validate the Issue AT (iat) is a mandatory parameter in JWT claim. When the CCA header request is sent without the "iat" claim and "maxTokenAge": 0 is set in /nrf/nf-common-component/v1/igw/ccaheader, the missing mandatory parameter is not validated, and the CCA header request is accepted by NRF.	The mandatory validation to be performed on the parameter would be missed at Ingress Gateway, and the request would be processed. **Workaround**: There is no workaround available.	3	23.2.0

Table 4-96 (Cont.) Ingress Gateway 24.2.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36464641	When feature Ingress Gateway POD Protection disabled at run time alerts are not getting cleared and metrics are getting pegged in NRF 23.4.0	When the Ingress Gateway Pod Protection feature is disabled at run time, alerts are not getting cleared and metrics are getting pegged in NRF 23.4.0.	Alerts are not getting cleared, and metrics would be pegged even when the feature is disabled during run time. **Workaround**: There is no workaround available.	3	23.4.0
35526243	Operational State change should be disallowed if the required pre-configurations are not present	Currently, the operational state at Ingress Gateway can be changed even if `thecontrolledshutdownerrormapping` and `errorcodeprofiles` are not configured. This indicates that the required action for rejecting traffic will not occur.	Requests will be processed by Igress Gateway when they are supposed to be rejected. **Workaround**: There is no workaround available.	3	23.3.0
34610831	IGW is accepting incorrect API names with out throwing any error	Ingress Gateway is accepting incorrect API names without displaying any error. If there is a typo in the configuration UDR, the command should get rejected. Otherwise, it indicates that the configuration is correct but the required behavior is not observed.	Non-existing resource name would be pretended to be successfully updated in the REST configuration. **Workaround**: There is no workaround available.	3	22.2.4

Table 4-96 (Cont.) Ingress Gateway 24.2.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36666519	Producer/ Consumer FQDN contain ":port" while messageCopy is enabled on GWs	For the header 3gpp sbi api root '3gpp-sbi-target-apiroot': 'http://RJBAR.UDCVMH.HSS02.UDM.5gc.mnc011.mcc724.3gppnetwork.org:8080'} The FQDN(both producer and consumer) should not contain port as per 3GPP specs. OBSERVATION: 'producer-fqdn': 'RJBAR.UDCVMH.HSS02.UDM.5gc.mnc011.mcc724.3gppnetwork.org:8080', EXPECTED: 'producer-fqdn': 'RJBAR.UDCVMH.HSS02.UDM.5gc.mnc011.mcc724.3gppnetwork.org',	Wrong metadata would be constructed at Ingress Gateway. **Workaround**: There is no workaround available.	4	23.4.0
35913189	Missing validation of the failureReqCountErrorCodeSeriesId mandatory parameter in the Ingress Gateway's Routes Configuration	As per the Oracle Communications Cloud Native Core, Network Slice Selection Function REST Specification Guide, failureReqCountErrorCodeSeriesId is a mandatory parameter for Routes Configuration in Ingress Gateway. When the failureReqCountErrorCodeSeriesId parameter is absent in the JSON payload, Ingress Gateway should reject the request.	Requests are processed by considering the mandatory configuration from the existing deployment configuration when it is not configured through REST APIs. **Workaround**: There is no workaround available.	4	23.3.0

4.3.14.6 Common Configuration Service Known Bugs

Common Configuration Service 24.2.0 Known Bugs

There are no known bugs in this release.

4.3.14.7 Helm Test Known Bugs

Release 24.2.0

There are no known bugs in this release.

4.3.14.8 NRF-Client Known Bugs

Release 24.2.0

There are no known bugs in this release.

4.3.14.9 App-Info Known Bugs

Release 24.2.0

There are no known bugs in this release.

4.3.14.10 Perf-Info Known Bugs

Perf-Info 24.2.0 Known Bugs

There are no known bugs in this release.

4.3.14.11 Debug Tool Known Bugs

Release 24.2.0

There are no known bugs in this release.