# Oracle® Communications

# Cloud Native Core Release Notes

Release 3.23.4

F89974-42

September 2024

Oracle Communications Cloud Native Core Release Notes, Release 3.23.4

F89974-42

# Contents

## 4 Resolved and Known Bugs

# 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 3.23.4 - F89974-42, September 2024**

**Policy 23.4.6 Release**

Updated the following sections with the details of Policy release 23.4.6:

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

**Release 3.23.4 - F89974-41, September 2024**

**CNE 23.4.6 Release**

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

**Release 3.23.4 - F89974-40, September 2024**

**cnDBTier 23.4.6 Release**

Added details about a feature enhancement in the Cloud Native Core cnDBTier section.

**Release 3.23.4 - F89974-39, August 2024**

**Policy 23.4.5 Release**

Updated the description for 36797796 bug in the Policy Resolved Bugs section.

**Release 3.23.4 - F89974-38, August 2024**

**cnDBTier 23.4.6 Release**

Updated the following sections with the details of cnDBTier release 23.4.6:

- Media Pack
- Compatibility Matrix
- cnDBTier Resolved Bugs

**Release 3.23.4 - F89974-37, August 2024**

**Policy 23.4.5 Release**

Removed the following bugs from the Policy Resolved Bugs section:

- 36824298
- 36722873

**Release 3.23.4 - F89974-36, August 2024**

**Policy 23.4.5 Release**

Updated the Policy section with details of *Support for DNN Exclusion* feature.

**Release 3.23.4 - F89974-34, August 2024**

**Policy 23.4.5 Release**

Updated the following sections with the details of Policy release 23.4.5:

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

**NRF 23.4.4 Release**

Updated the following sections with the details of NRF release 23.4.4:

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

**Release 3.23.4 - F89974-33, July 2024**

**CNE 23.4.6 Release**

Updated the following sections with the details of CNE release 23.4.6:

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

**Release 3.23.4 - F89974-32, July 2024**

**BSF 23.4.4 Release**

Updated the following sections with the details of BSF release 23.4.4:

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

**Release 3.23.4 - F89974-31, July 2024**

**Console 23.4.2 Release**

Updated the following sections with the details of Console release 23.4.2:

- Media Pack

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

**UDR 23.4.2 Release**

Updated the following sections with the details of UDR release 23.4.2:

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

**Release 3.23.4 - F89974-30, July 2024**

**cnDBTier 23.4.5 Release**

Updated the following sections with the details of cnDBTier release 23.4.5:

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

**NEF 23.4.4 Release**

Updated the following sections with the details of NEF release 23.4.4:

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

**NRF 23.4.3 Release**

Updated the following sections with the details of NRF release 23.4.3:

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

**SCP 23.4.3 Release**

Updated the following sections with the details of SCP release 23.4.3:

- Media Pack
- Compatibility Matrix
- Common Microservices Load Lineup

- SCP Security Certification Declaration
- SCP Resolved Bugs

**SEPP 23.4.2 Release**

Updated the following sections with the details of SEPP release 23.4.2:

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

### Release 3.23.4 - F89974-28, July 2024

**Policy 23.4.4 Release**

Updated the following sections with the details of Policy release 23.4.4:

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

### Release 3.23.4 - F89974-27, July 2024

**Policy 23.4.x Release**

Updated the Compatibility Matrix section with supported CNE and Kubernetes versions for Policy 23.4.x.

**BSF 23.4.x Release**

Updated the Compatibility Matrix section with supported CNE and Kubernetes versions for BSF 23.4.x.

**OCCM 23.4.3 Release**

Updated the following sections with the details of OCCM 23.4.3:

- Common Microservices Load Lineup
- Security Certification Declaration

### Release 3.23.4 - F89974-26, May 2024

**cnDBTier 23.4.4 Release**

Updated the following sections with the details of cnDBTier release 23.4.4:

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

**cnDBTier 23.4.3 Release**

Updated the known bug details for 23.4.3 in the cnDBTier Known Bugs section.

### Release 3.23.4 - F89974-25, May 2024

#### OSO 23.4.5 Release

Updated the following sections with the details of OSO release 23.4.5:

- OSO
- Media Pack
- Compatibility Matrix

### Release 3.23.4 - F89974-24, April 2024

#### SEPP 23.4.1 Release

Updated the following sections with the details of SEPP CPU Patch 23.4.1:

- Security Edge Protection Proxy (SEPP)
- SEPP Resolved Bugs
- SEPP Known Bugs

### Release 3.23.4 - F89974-23, April 2024

#### CNE 23.4.4 Release

Updated the following sections with the details of CNE release 23.4.4:

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

#### OSO 23.4.4 Release

Updated the following sections with the details of OSO release 23.4.4:

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

#### Policy 23.4.3 Release

Updated the following sections with the details of Policy release 23.4.3:

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

#### BSF 23.4.2 Release

Updated the following sections with the details of BSF release 23.4.2:

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

**Release 3.23.4 - F89974-22, April 2024**

**cnDBTier 23.4.3 Release**

Updated the following sections with the details of cnDBTier release 23.4.3:

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

**NEF 23.4.3 Release**

Updated the following sections with the details of NEF release 23.4.3:

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

**Release 3.23.4 - F89974-21, April 2024**

**NRF 23.4.2 Release**

Updated the following section with the details of NRF release 23.4.2:

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

**SCP 23.4.2 Release**

Updated the following sections with the details of SCP release 23.4.2:

- Media Pack
- Compatibility Matrix
- 3GPP Compatibility Matrix
- Common Microservices Load Lineup
- SCP Security Certification Declaration

- SCP Resolved Bugs

**SEPP 23.4.1 Release**

Updated the following sections with the details of SEPP release 23.4.1:

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

**UDR 23.4.1 Release**

Updated the following sections with the details of UDR release 23.4.1:

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

### Release 3.23.4 - F89974-20, April 2024

**CNC Console 23.4.1 Release**

Updated the following sections with the details of CNC Console release 23.4.1:

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

### Release 3.23.4 - F89974-19, April 2024

**OCCM 23.4.2 Release**

Updated the following sections with the details of OCCM release 23.4.2:

- Media Pack
- Compatibility Matrix
- 3GPP Compatibility Matrix
- Common Microservices Load Lineup
- Security Certification Declaration

### Release 3.23.4 - F89974-17, April 2024

**NRF 23.4.1 Release**

- Added 36137134 bug in the NRF Resolved Bugs section.
- Added 36366551 bug in the NRF Known Bugs section.

**Release 3.23.4 - F89974-16, March 2024**

**Policy 23.4.2 Release**

Updated the following sections with the details of Policy release 23.4.2:

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

**NEF 23.4.2 Release**

Updated the following sections with the details of NEF release 23.4.2:

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

**Release 3.23.4 - F89974-15, March 2024**

**OCCM 23.4.1 Release**

Updated the following sections with the details of OCCM release 23.4.1:

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

**Release 3.23.4 - F89974-14, March 2024**

**NRF 23.4.1 Release**

Updated the following section with the details of NRF release 23.4.1:

- 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

**Release 3.23.4 - F89974-13, March 2024**

**UDR ATS 23.4.2 Release**

Updated the following section with the details of UDR ATS release 23.4.2:

- Media Pack
- UDR Resolved Bugs

**Release 3.23.4 - F89974-12, February 2024**

**SCP 23.4.1 Release**

Updated the following sections with the details of SCP release 23.4.1:

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

**Release 3.23.4 - F89974-11, February 2024**

**cnDBTier 23.4.2 Release**

Updated the following sections with the details of cnDBTier release 23.4.2:

- Media Pack
- Compatibility Matrix
- cnDBTier Resolved Bugs

**CNE 23.4.1 Release**

Added a known bug for CNE 23.4.1 in the CNE Known Bugs section.

**Release 3.23.4 - F89974-10, February 2024**

**CNE 23.4.1 Release**

Updated the following sections with the details of CNE release 23.4.1:

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

**Policy 23.4.1 Release**

Updated the following sections with the details of Policy release 23.4.1:

- Media Pack

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

**SEPP 23.4.0 Release**

Added the "Separate Port Configurations for N32c and N32f on the Egress Routes" feature from the Security Edge Protection Proxy (SEPP) feature section.

### Release 3.23.4 - F89974-09, February 2024

**NRF ATS 23.4.1 Release**

Updated the following sections with the details of NRF ATS release 23.4.1:

- Media Pack
- Common Microservices Load Lineup
- NRF Resolved Bugs

### Release 3.23.4 - F89974-08, February 2024

**cnDBTier 23.4.1 Release**

Updated the following sections with the details of cnDBTier release 23.4.1:

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

### Release 3.23.4 - F89974-07, January 2024

**SCP 23.4.0 Release**

> **Note:**
>
> Oracle Communications Cloud Native Core Release 2.23.3 is the final release supporting the SCP Reverse Proxy and Transparent Proxy mode features. Subsequently, these features are no longer supported from Service Communication Proxy 23.4.0 onwards.

**UDR ATS 23.4.1 Release**

Added resolved bugs in the UDR Resolved Bugs section.

**NEF 23.4.1 Release**

Updated the following sections with the details of NEF release 23.4.1:

- Media Pack
- Compatibility Matrix
- Common Microservices Load Lineup

- Security Certification Declaration
- NEF Resolved Bugs

**BSF 23.4.1 Release**

Updated the following sections with the details of BSF release 23.4.1:

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

### Release 3.23.4 - F89974-06, January 2024

**SCP 23.4.0 Release**

Added a known bug in the SCP Known Bugs section.

### Release 3.23.4 - F89974-05, January 2024

**SCP 23.4.0 Release**

Updated the following sections with the details of SCP release 23.4.0:

- 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 3.23.4 - F89974-04, January 2024

**SEPP 23.4.0 Release**

Removed the "Separate Port Configurations for N32c and N32f on the Egress Routes" feature from the Security Edge Protection Proxy (SEPP) feature section.

### Release 3.23.4 - F89974-03, January 2024

**CDCS 23.4.0 Release**

Updated the following sections with the details of CDCS release 23.4.0:

- Continuous Delivery Control Server (CDCS)
- Media Pack
- Compatibility Matrix
- 3GPP Compatibility Matrix
- CDCS Resolved Bugs
- CDCS Known Bugs

### Release 3.23.4 - F89974-02, December 2023

**BSF 23.4.0 Release**

Updated the following sections with the details of BSF release 23.4.0:

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

**Policy 23.4.0 Release**

Updated the following sections with the details of Policy release 23.4.0:

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

### Release 3.23.4 - F89974-01, December 2023

**CNC Console 23.4.0 Release**

Updated the following sections with the details of CNC Console release 23.4.0:

- Cloud Native Configuration Console (CNC Console)
- Media Pack
- Compatibility Matrix
- Common Microservices Load Lineup
- CNC Console Security Certification Declaration
- CNC Console Resolved Bugs

**CNE 23.4.0 Release**

Updated the following sections with the details of CNE release 23.4.0:

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

**cnDBTier 23.4.0 Release**

Updated the following sections with the details of cnDBTier release 23.4.0:

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

**NEF 23.4.0 Release**

Updated the following sections with the details of NEF release 23.4.0:

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

**NRF 23.4.0 Release**

Updated the following sections with the details of NRF release 23.4.0:

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

**NSSF 23.4.0 Release**

Updated the following sections with the details of NSSF release 23.4.0:

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

**OCCM 23.4.0 Release**

Updated the following sections with the details of OCCM release 23.4.0:

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

**SEPP 23.4.0 Release**

Updated the following sections with the details of SEPP release 23.4.0:

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

**UDR 23.4.0 Release**

Updated the following sections with the details of UDR release 23.4.0:

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

**Common Services Resolved Bugs**

Updated the following sections with the details of Common Services Resolved Bugs for release 23.4.0:

- ATS Resolved Bugs
- Egress Gateway Resolved Bugs
- Ingress Gateway Resolved Bugs
- Helm Test Resolved Bugs
- Mediation Resolved Bugs

**Common Services Known Bugs**

Updated the following sections with the details of Common Services Known Bugs for release 23.4.0:

- Egress Gateway Known Bugs
- Ingress Gateway Known Bugs

# 1 Introduction

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

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

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

# 2
# Feature Descriptions

This chapter provides a summary of new features and updates to the existing features for network functions released in Cloud Native Core release 3.23.4.

## 2.1 Automated Testing Suite (ATS) Framework

**Release 23.4.0**

Oracle Communications Cloud Native Core, Automated Test Suite (ATS) framework 23.4.0 has been updated with the following enhancements:

- **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 *"Support for Transport Layer Security"* in *Oracle Communications Cloud Native Core, Automated Test Suite Guide*.
- **ATS Feature Activation and Deactivation**: This feature allows users to activate or deactivate specific features within the ATS using Helm charts. For more information, see *"ATS Feature Activation and Deactivation"* in *Oracle Communications Cloud Native Core, Automated Test Suite Guide*.
- **Individual Stage Group Selection**: This feature allows users to select and execute a single or multiple stages or groups by selecting a check box for the corresponding stage or group. For more information, see *"Individual Stage Group Selection"* in *Oracle Communications Cloud Native Core, Automated Test Suite Guide*.

## 2.2 Binding Support Function (BSF)

**Release 23.4.4**

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

**Release 23.4.2**

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

**Release 23.4.1**

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

**Release 23.4.0**

Oracle Communications Cloud Native Core, Binding Support Function (BSF) 23.4.0 has been updated with the following enhancements:

- **Diameter Session Retry for Rx AAR Messages**: BSF sends the Rx AAR diameter messages toward the PCF Diameter Gateway. This feature enables BSF to retry sending the failed Rx AAR diameter messages. The operator can attempt to resend failed diameter message for Rx diameter interface using CNC Console configurations. For more information about the feature, see *"Diameter Session Retry"* section in *Oracle Communications Cloud Native Core, Binding Support Function User Guide*.

- **Support for BSF Status on NRF on CNC Console**: This features enables Operator to check the following status on BSF CNC Console:
  - BSF registered NF profile and its status on NRF
  - Currently active, primary, secondary, or any other alternate NRF instances status. For more information about the feature, see *"Support for BSF Status on NRF on CNC Console"* section in *Oracle Communications Cloud Native Core, Binding Support Function User Guide*.
- **Migration from opentracing to OpenTelemetry**: OpenTelemetry automatic instrumentation has been implemented to show similar traces as Open Tracing in Jaeger UI. For more details, see "Tracing Configurations" in Oracle Communications Cloud Native Core, BSF Installation, Upgrade, and Fault Recovery Guide.

> **Note:**
>
> Preupgrade consideration: When upgrading from 23.2.0 to 23.4.0, certain scenarios needs to be considered. For more information, see *"Preupgrade Tasks"* in *Oracle Communications Cloud Native Core, BSF Installation, Upgrade, and Fault Recovery Guide*.

- **Enhancements to discard policy for diameter sessions**: Discard policy for diameter sessions is enhanced with options to discard sessions based on priority and priority percentage. For more information, see *"Load Shedding Profiles"* section in *Oracle Communications Cloud Native Core, Binding Support Function User Guide*.
- **Support for Network Policies**: Network Policies are an application-centric construct that allows to specify how a pod communicates with various network entities. It creates pod-level rules to control communication between the cluster's pods and services, and to determine which pods and services can access one another inside a cluster. For more information, see *"Network Policies"* section in *Oracle Communications Cloud Native Core, Binding Support Function User Guide*.
- **ATS Feature Activation and Deactivation**: This feature allows to activate or deactivate the specific features within the ATS using Helm charts. Once these features are removed, they cannot be reinstated in the deployed ATS. However, users have the option to reinstall the ATS to restore the disabled features. For more information about the feature, see *"ATS Feature Activation and Deactivation"* section in *Oracle Communications Cloud Native Core, Automated Testing Suite Guide*.

## 2.3 Continuous Delivery Control Server (CDCS)

**Release 23.4.0**

Oracle Communications CD Control Server (CDCS) 23.4.0 has been updated with the following enhancements:

- **Support for updating Oracle Linux**: CDCS allows to update the base Oracle Linux version for CDCS VMs and the host OS (when CDCS is installed on a BareMetal server) with the latest version (9.x). For more information about the Oracle Linux version, see the *Oracle Communications CD Control Server Installation and Upgrade Guide.*
- **Support for CNE releases**: CDCS supports the installation and upgrade of CNE releases 23.1.x, 23.2.x, 23.3.x, and 23.4.0. A specific release can be installed by selecting the

supported release versions while running the **Install OCCNE** and **Upgrade OCCNE** commands. For more information about selecting the versions, see the "*Managing CNE*" section in *Oracle Communications CD Control Server User Guide.*

- **Support for CNE backup and restore**: CDCS helps to take a backup of CNE using the **Schedule OCCNE Backup** command and restore CNE using the **Restore OCCNE** command at any managed site. For more information about this feature, see the "*Managing CNE*" section in *Oracle Communications CD Control Server User Guide.*
- **Support for new installation options**: CDCS now supports the use of custom configurable volumes for the Bootstrap and other CNE VMs for storage on OpenStack. For more information, see the *Oracle Communications CD Control Server Installation and Upgrade Guide.*
- **Support for new commands**: CDCS supports the following new commands:
  - Activate OCCNE Backup Feature
  - Activate OCCNE Local DNS Feature
  - Configure OCCNE Backup
  - Restore OCCNE

  For more information about the new commands, see the sections *"Activating CNE Backup Feature ", "Activating CNE Local DNS Feature", "Creating CNE Backup",* and *"Restoring CNE from Backup"* in *Oracle Communications CD Control Server User Guide.*

For more details about the features released in CDCS 23.4.x, see *Oracle Communications CD Control Server User Guide.*

## 2.4 Cloud Native Core cnDBTier

**Release 23.4.6**

Oracle Communications Cloud Native Core, cnDBTier (cnDBTier) 23.4.6 has been updated with the following enhancement:

- **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:
  - 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*.

**Release 23.4.5**

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

**Release 23.4.4**

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

**Release 23.4.3**

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

### Release 23.4.2

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

### Release 23.4.1

Oracle Communications Cloud Native Core, cnDBTier (cnDBTier) 23.4.1 has been updated with the following enhancements:

- **TLS Support for Georeplication:** With this feature, cnDBTier automates the process of configuring TLS for georeplication between cnDBTier sites. On enabling this feature, the replication SQL pod uses the certificates provided or configured to establish an encrypted connection for georeplication. This ensures that the replication data transfer is secure. For more information about this feature, see *Oracle Communications Cloud Native Core, cnDBTier User Guide* and *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*.
  **Consideration:** If you are enabling TLS for the replication channels in this release, be informed about the following conditions:
  - You can't roll back from 23.4.1 to previous releases.
  - You cannot upgrade from 23.4.1 to any future versions of 23.4.x. However, cnDBTier plans to resolve this upgrade restriction in a future release.
- **dbtrecover Support for Georeplication Recovery Between Different cnDBTier Versions:** With this feature, the `dbtrecover` script supports georeplication recovery between sites that are running on different cnDBTier versions. For more information about this feature, see the "Recovering Georeplication Sites Using dbtrecover" section in *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*.
  **Consideration:** Consider the following conditions before using the `dbtrecover` script for performing a georeplication recovery between sites running on different cnDBTier versions:
  - The script supports georeplication recovery between sites only in the following cases:
    - The good site and the bad site (the site to be recovered) run the same cnDBTier version.
    - The good site runs a lower cnDBTier version. However, the cnDBTier release on both the good site and the bad site supports the same database replication REST API.
  - The script doesn't support georeplication recovery between sites in the following cases:
    - The good site runs a cnDBTier version that is higher than the version on the bad site.
    - The good site runs a lower cnDBTier version and uses a different database replication REST API from the one used by the bad site.
  - The following cnDBTier versions use the old database replication API:
    - cnDBTier versions below 22.4.2
    - cnDBTier version 23.1.0
  - The following cnDBTier versions use the new database replication API:
    - cnDBTier versions greater than or equal to 22.4.2 and less than 23.1.0
    - cnDBTier version greater than or equal to 23.1.1

**Release 23.4.0**

Oracle Communications Cloud Native Core, cnDBTier (cnDBTier) 23.4.0 has been updated with the following enhancements:

- **REST APIs to Display cnDBTier Data on CNC Console**: In this release, cnDBTier provides the following REST APIs to CNC Console:
  - Backup list
  - Database statistic reports
  - Replication heartbeat status
  - On-demand backup

  CNC Console uses these REST APIs to fetch cnDBTier data and display them on the CNC Console GUI. This way, cnDBTier facilitates users to integrate cnDBTier on CNC Console and allows users to perform cnDBTier read operations such as checking the list of completed backups and overall heartbeat status. For more information about the feature and the REST APIs, see *Oracle Communications Cloud Native Core, cnDBTier User Guide*.
- **Network Policies**: With this release, cnDBTier supports network policies to restrict incoming and outgoing network traffic. This ensures security and isolation of cnDBTier services in Kubernetes clusters. For more information about enabling and configuring this feature, see *Oracle Communications Cloud Native Core, cnDBTier User Guide* and *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*.
- **Support for New Versions of Software**: cnDBTier has updated the following software in this release:
  - Oracle MySQL Cluster Database - 8.0.35
  - Spring Boot - 3.1.5
- **TLS Support for Georeplication**: cnDBTier 23.4.0 doesn't support Transport Layer Security (TLS). Therefore, the feature is disabled in this release by default. Follow the updated procedures in the documents to avoid encountering errors while performing any operation. For the updated procedures, see *Oracle Communications Cloud Native Core, cnDBTier User Guide* and *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*.

## 2.5 Cloud Native Configuration Console (CNC Console)

**Release 23.4.2**

There are no new features or enhancements in this release.

**Release 23.4.1**

There are no new features or enhancements in this release.

**Release 23.4.0**

Oracle Communications Cloud Native Configuration Console (CNC Console) 23.4.0 has been updated with the following enhancements:

- **Support for cnDBTier**: The CNC Console GUI now supports cnDBTier READ operations and enables the cnDBTier Menu for the Console. This feature incorporates authentication and authorization for API and GUI requests, along with the inclusion of metrics, alerts, and KPIs. For more information, see *Oracle Communications Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide* and *Oracle Communications Cloud Native Configuration Console User Guide*.

- **Support for OCCM**: CNC Console supports Oracle Communications Cloud Native Core, Certificate Management (OCCM). OCCM is an automated solution for managing the certificates needed for Oracle 5G Network Functions (NFs). As part of CNC Console and OCCM integration, features such as authentication, authorization of API/GUI requests, metrics, alerts, KPIs are now supported. For more information, see *Oracle Communications Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide* and *Oracle Communications Cloud Native Configuration Console User Guide*.
- **NF Versions Supported by CNC Console**: The following NF versions are supported in this release:
  - SCP - 23.4.x
  - NRF - 23.4.x
  - UDR - 23.4.x
  - POLICY - 23.4.x
  - BSF - 23.4.x
  - SEPP - 23.4.x
  - NSSF - 23.4.x
  - OCNADD - 23.4.x
  - OCNWDAF - 23.4.x
  - PROVGW - 23.4.x

## 2.6 Cloud Native Environment (CNE)

> **Note:**
>
> The procedure to update OpenStack credentials is revised in the 23.4.6 User Guide. If you are updating OpenStack credentials on other versions of 23.4.x, refer to the latest procedure from 23.4.6 *Oracle Communications Cloud Native Core, Cloud Native Environment User Guide*.

**Release 23.4.6**

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

**Release 23.4.4**

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

**Release 23.4.1**

Oracle Communications Cloud Native Core, Cloud Native Environment (CNE) 23.4.1 has been updated with the following enhancements:

- **Upgrade Support from 23.3.x and 23.4.0**: CNE 23.4.0 was released as an installation-only version. To overcome this limitation, CNE 23.4.1 is developed to support upgrade from

23.3.x and 23.4.0. While upgrading from 23.3.x, CNE uplifts the version of the following components:

- Kubernetes control plane is uplifted to 1.27.x
- Oracle Operating System (OS) on all CNE nodes and Load Balancer Virtual Machines (LBVMs) are uplifted to Oracle Linux 9

**Release 23.4.0**

Oracle Communications Cloud Native Core, Cloud Native Environment (CNE) 23.4.0 has been updated with the following enhancements:

- **Oracle Linux Version Uplift**: In this release, Oracle Linux is uplifted from version 8 to version 9.2. As part of this uplift, all the hosts provisioned in CNE are installed with Oracle Linux 9.2 operating system. This includes CNE cluster nodes, LoadBalancer, and Bastion Hosts. Container images that are built as part of CNE development bastion-controller and lb-controller are also built using Oracle Linux 9.2 base image. Third-party container images used in CNE including Oracle OpenSearch and Oracle OpenSearch Dashboard container images are not part of this uplift.

  > **Note:**
  >
  > Oracle Linux version uplift has no impact on NF container image versions. NFs can continue to use the same version of image, as the changes made in Oracle Linux are backward compatible with the NF container image versions.

- **New Versions of Common Services**: The following common services are upgraded in this release:
  - Helm - 3.12.3
  - Kubernetes - 1.27.5
  - containerd - 1.7.5
  - Calico - 3.25.2
  - MetalLB - 0.13.11
  - Prometheus - 2.44.0
  - Grafana - 9.5.3
  - Jaeger - 1.45.0
  - Istio - 1.18.2
  - Kyverno - 1.9.0
  - cert-manager - 1.12.4
  - Oracle OpenSearch 2.3.0
  - Oracle OpenSearch Dashboard 2.3.0
  - Fluentd - opensearch 1.16.2
  - Velero 1.12.0

  To get the complete list of third-party services and their versions, refer to the `dependencies_23.4.0.tgz` file provided as part of the software delivery package.

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

- **Upgrade Consideration**: CNE 23.4.0 is an installation only release and doesn't support upgrade from any previous releases.

**Operations Services Overlay (OSO)**

**Release 23.4.5**

Oracle Communications Operations Services Overlay 23.4.5 has been updated with the following enhancements:

- the version of 23_4_common_pod is updated to 23.4.5.
- OSO roll back is supported to previous versions.

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

**Release 23.4.4**

Oracle Communications Operations Services Overlay 23.4.4 has been updated with the following enhancements:

Support for new versions:

- Prometheus version is uplifted from version 0.26.1 to 0.50.1.
- configmap-reload version is uplifted from v0.8.0 to 0.12.0.
- nginx/controller is replaced with 23_4_common9_pod:latest.

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

**Release 23.4.0**

Oracle Communications Operations Services Overlay 23.4.0 has been updated with the following enhancements:

Support for new versions:

- AlertManager version is uplifted from version 0.25 to 0.26.1.
- nginx version is uplifted from v1.5.1 to 1.9.4.

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

## 2.7 Network Exposure Function (NEF)

**Release 23.4.4**

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

**Release 23.4.3**

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

### Release 23.4.2

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

### Release 23.4.1

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

### Release 23.4.0

Oracle Communications Cloud Native Core, Network Exposure Function (NEF) 23.4.0 has been updated with the following enhancements:

- **Converged Charging Support in NEF**: This feature enables the NEF to invoke its northbound API for charging purposes. This allows NEF to communicate with CHF NF to perform any charging related functionalities. It can be used to gather the necessary data for various management activities, such as credit control, accounting, billing, and statistics. For more information, see *Oracle Communications Cloud Native Core, Network Exposure Function User Guide* and *Oracle Communications Cloud Native Core, Network Exposure Function Installation, Upgrade, and Fault Recovery Guide*.
- **Support for Update Operation in Monitoring Event**: This feature enables NEF to support PUT operation for Monitoring Event Service (3gpp-monitoring-event). For more information, see *Oracle Communications Cloud Native Core, Network Exposure Function User Guide.*

## 2.8 Network Repository Function (NRF)

This section explains the features or enhancements performed for Oracle Communications Cloud Native Core, Network Repository Functions (NRF).

### Release 23.4.4

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

### Release 23.4.3

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

### Release 23.4.2

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

### Release 23.4.1

Oracle Communications Cloud Native Core, Network Repository Functions (NRF) 23.4.1 has been updated with the following enhancements:

- **Support for Service Level Priority with same Service Names**: The Preferred Locality priority handling has been enhanced to support service level priority with the same service names. For service-name based discovery query, NRF updates the profile level priority and service level priority of the NF profile if there are multiple services in the NF profile with the same service name after processing the discovery query. For more information about the feature, see "Preferred Locality" in *Oracle Communications Cloud Native Core, Network Repository Function User Guide*.

**Release 23.4.0**

Oracle Communications Cloud Native Core, Network Repository Functions (NRF) 23.4.0 has been updated with the following enhancements:

- **Support for Automated Certificate Lifecycle Management:** NRF supports automated certificate lifecycle management when integrated with Oracle Communications Cloud Native Core, Certificate Management (OCCM) in compliance with 3GPP security recommendations. For more information about automated certificate management, see *"Support for Automated Certificate Lifecycle Management"* in *Oracle Communications Cloud Native Core, Network Repository Function User Guide*.
- **Support for `vsmf-support-ind` Attribute in NF Discover Service Operation:** NRF supports `vsmf-support-ind attribute` in the NF Discover service operation query as per the 3GPP standards. For more information about the attribute, see NRF Compliance Matrix.
- **Support for cnDBTier APIs in CNC Console:** With this enhancement, cnDBTier APIs are integrated into the CNC Console, and users can view specific cnDBTier statuses on the CNC Console. For more information, see *"Support for cnDBTier APIs in CNC Console"* in *Oracle Communications Cloud Native Core, Network Repository Function User Guide*.
- **Routing Egress Messages through SCP:** NRF supports routing of the following Egress requests through SCP:
  - SLF requests
  - Notification requests
  - NRF Forwarding requests
  - Roaming requests

  This feature provides the flexibility to independently configure the Egress requests routing either directly or through SCP. For more information about routing messages through SCP, see *"Routing Egress Messages Through SCP"* in *Oracle Communications Cloud Native Core, Network Repository Function User Guide.*
- **Enhanced NRF Set Based Deployment (NRF Growth)**: NRF supports multiple NRF sets deployment in a network to support increased traffic and expand the capacity of the network. Each NRF in a set synchronizes with the most preferred NRF of the other sets to retrieve the state data of that set. Thus, every NRF has the complete segment-level view of all the sets in the specific segment. When the feature is enabled, NRF core microservices fetch the state data of the remote NRF sets from Cache Data Service. For more information about the feature, see *Oracle Communications Cloud Native Core, Network Repository Function User Guide*.
- **Support for Cache Data Service:** A new microservice, Cache Data Service (CDS) is deployed by default. The Cache Data Service (CDS) builds and maintains state data of local and remote NRF sets in its in-memory cache. This state data is read by other NRF core microservices for various service operations. For more information about the CDS, see *Oracle Communications Cloud Native Core, Network Repository Function User Guide*.
  **Installation and Upgrade Considerations**:
  - Upon 23.4.0 installation or upgrade, the CDS microservice pod is deployed by default. The NRF core microservices query the CDS for state data information. In case CDS is not available, NRF core microservices fall back to the cnDBTier for service operation.
  - Release 23.3.x microservice pods retrieve the state data from the cnDBTier for processing the service operations.

  - Release 23.4.x microservice pods retrieve queries CDS to retrieve the state data for processing the service operations.
  - In case of in-service upgrade:
    - CDS updates its in-memory cache with state data. The readiness probes of the CDS are configured to succeed only after at least one cache update attempt is performed. The cache is updated with the local NRF set data from the cnDBTier and if the growth feature is enabled the cache is updated with remote NRF set data.
    - During the above-mentioned upgrade scenario, until the nrfCacheData pod is available, the previous and new release pods of other microservices will query the old release pod of the CDS for the state data. This will ensure there are no in-service traffic failures during the upgrade.

## 2.9 Network Slice Selection Function (NSSF)

**Release 23.4.0**

Oracle Communications Cloud Native Core, Network Slice Selection Function (NSSF) 23.4.0 has been updated with the following enhancements:

- **LCI and OCI Headers**: In the 5G architecture, frequent network overload resulting from substantial data exchanges between Producer and Consumer Network Functions (NFs) necessitates load balancing to prevent failures. This feature introduces LCI and OCI Headers in NSSF, collectively offering real-time insights into NSSF resources and enabling efficient traffic management. These headers, by providing load and overload information, not only facilitate optimized traffic distribution but also enable proactive measures to prevent network failures caused by overload scenarios. For more information, see *"LCI and OCI Headers"* section in *Oracle Communications Cloud Native Core, Network slice Selection Function User Guide*.
- **Server Header in NSSF**: NSSF in 5G handles security aspects and manages requests from various network functions (NFs) and entities via HTTP. When errors occur, consumer NFs need to identify the source of the issue for troubleshooting. This feature adds support for Server Headers in NSSF responses, which is useful in identifying the type and origin of an error. This enhancement improves NSSF's error handling for better troubleshooting and corrective actions by the consumer NFs. For more information, see *"Server Header in NSSF"* section in *Oracle Communications Cloud Native Core, Network slice Selection Function User Guide*.

## 2.10 Oracle Communications Cloud Native Core, Certificate Management (OCCM)

**Release 23.4.3**

There are no new features or enhancements in this release.

**Release 23.4.2**

There are no new features or enhancements in this release.

**Release 23.4.1**

There are no new features or enhancements in this release.

**Release 23.4.0**

Oracle Communications Cloud Native Core, Certificate Management (OCCM) 23.4.0 has been updated with the following enhancements:

- **PKI Automation and Certificate Management**: Oracle Communications Cloud Native Core, Certificate Management (OCCM) is an automated solution for managing the certificates needed for Oracle 5G Network Functions (NFs). OCCM constantly monitors and renews the certificates based on their validity or expiry period. OCCM integrates with the Certificate Authority(s) using Certificate Management Protocol Version 2 (CMPv2) and RFC4210 to facilitate these certificate management operations:
  - Operator-initiated certificate creation
  - Operator-initiated certificate recreation
  - Automatic certificate monitoring and renewal

  OCCM supports transport of CMPv2 messages using HTTP-based protocol. OCCM provides the following mechanisms to establish initial trust between OCCM and CA(s):
  - Certificate-based message signing
  - Pre-shared key or MAC based authentication

  All the subsequent CMPv2 procedures are authenticated using the certificate-based mechanism in compliance with 3GPP TS 33.310.

  The keys and X.509 certificates are managed using Kubernetes secrets. For more information, see *Oracle Communications Cloud Native Core, Certificate Management Installation, Upgrade, and Fault Recovery Guide* and *Oracle Communications Cloud Native Core, Certificate Management User Guide*.
- **OCCM Deployment Models**: OCCM provides the following deployment models to support certificate management for the integrated NF(s) instantiated within the same cluster:
  - Dedicated deployment model - OCCM resides in the same Kubernetes namespace as the NF or Components.
  - Shared deployment model - OCCM is deployed in a separate Kubernetes namespace and can manage certificates of multiple NFs or components deployed in other Kubernetes namespaces.

  Appropriate permissions must be assigned to OCCM using Kubernetes Service Account, Role, and Role Binding, based on the selected deployment model. For more information, see *Oracle Communications Cloud Native Core, Certificate Management Installation, Upgrade, and Fault Recovery Guide*.
- **Console support for OCCM Configuration**: Console support for OCCM configuration is enabled. OCCM configuration can be performed through Console GUI or by invoking REST API by passing Console Access Token. Following OCCM GUI screens are supported at Console:
  - Issuer Configuration
  - Certificate Configuration
  - Logging Configuration
- **Configure Kubernetes Network Policies**: OCCM has implemented the Network policies framework to enable the user to specify how a pod communicates with network entities. It enables OCCM to create pod-level rules needed for OCCM data flows, to manage Ingress and Egress traffic.

- **Support for OCCM Deployment using Continuous Delivery Control Server (CDCS):** In addition to OCCM's Command Line Interface (CLI) deployment method, OCCM can be deployed using the Continuous Delivery Control Server (CDCS), which is a centralized server that automates OCCM deployment processes such as downloading the OCCM package, installation, upgrade, and rollback. For more information about CDCS, see *Oracle Communications Cloud Native Core, CD Control Server User Guide.* For information about OCCM deployment using CDCS, see the *"Overview"* section in *Oracle Communications Cloud Native Core, Certificate Management Installation, Upgrade, and Fault Recovery Guide*.

## 2.11 Policy

**Release 23.4.6**

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

**Release 23.4.5**

Oracle Communications Cloud Native Core, Converged Policy 23.4.5 has been updated with the following enhancement:

- **Support for DNN Exclusion**: The communication from SM service with Binding service, Bulwark service, and PDS can be skipped based on the DNN using a few advanced settings configurations, *USER.allDataTypes.excludeDnns, BINDING.excludeDnns*, and *BULWARK.excludeDnns* in SM service.
  For more information, see *Support for DNN Exclusion* section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.

**Release 23.4.4**

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

**Release 23.4.3**

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

**Release 23.4.2**

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

**Release 23.4.1**

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

**Release 23.4.0**

Oracle Communications Cloud Native Core, Converged Policy 23.4.0 has been updated with the following enhancements:

- **Bulwark Pod Congestion Control:** Bulwark, a Policy microservice provides distributed lock mechanism using distributed coherence. The traffic at bulwark service is high as all the consumer services use its distributed lock mechanism to handle concurrent transactions. In the production environment, the bulwark pods must be protected from traffic congestion. Bulwark pod congestion control functionality helps in regulating the traffic and improves its service availability. For more information, see *Bulwark Pod Congestion Control* section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.

- **PCF UE service with New Error Fields for N1 Message Retransmission:** This feature supports UePolicy-Max Number of Re-transmissions to be separately configure for each error type on the GUI. For more information, see *UE Policy Enhancements* section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.
- **Support of Policy evaluation on AMF Notification on N1Notify and N1N2NotifyFailure:** This feature supports PCF to evaluate Policies and take actions when PCF receives notification such as N1Notify with "command complete" or "command reject" or N1N2Transfer failure notification messages from AMF. For more information, see *UE Policy Enhancements* section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.
- **Support of Policy Action to send the Notify Terminate for AM/UE Service:** This feature supports PCF to initiate Policy association termination toward core services (AM/SM/UE) because of notifications coming from UDR or CHF or due to updates coming from AMF/SMF. The initiation of Policy association termination is based on policy evaluation by PRE and policy action that is configured. For more information, see *Support of Policy Action to Send the Notify Terminate* section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.
- **Diameter Session Retry:** This feature is enhanced to support following multiple configurations in CNC Console to handle session retries on Rx interface:
  - Number of session retries configuration
  - Error handling based on error origination peer configurations.

  For more information, see *Diameter Session Retry* section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.
- **Supports UDR Discovery using Group Id**: This feature enables PCF to perform UDR discovery using query parameter "group-id-list" during SM, AM, and UE Policy associations. PCF receives the UDR group id from AMF/SMF services as part of its header requests. From this header, PCF extracts the UDR group id and uses it to discover UDR. With this feature implementation the number of discovery requests to NRF for the same UDR is reduced. For more information, see *Supports UDR Discovery using Group Id* section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.
- **RAA Error Code Handling:** This feature helps in error handling at SM and PA service where on receipt of error response from Diameter Connector for initiated update-notify or RAR message the operator should be able to take corrective actions. For more details, see *"RAA Error Code Handling"* section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.
- **Support of SUPI-based NRF Discovery Optimization and Response Caching from UDR:** This feature helps in optimizing SUPI based NRF discoveries between the query and subscription (GET and POST) of the policy data request towards UDR. It is applicable only for SUPI based discovery queries towards UDR. For more details, see *"Support of SUPI-based NRF Discovery Optimization and Response Caching from UDR"* section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.
- **PCF must STOP sending Update Notify on N7 when PCC Rule has Flow Status set to 'REMOVED':** CNC Policy is enhanced to support SM create when it contains flow status set as 'removed' for any of the media components. For more details, see *"Support for Resource Allocation for PCC Rules"* section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.
- **Migration from opentracing to OpenTelemetry:** OpenTelemetry automatic instrumentation has been implemented to show similar traces as Open Tracing in Jaeger UI. For more details, see "*Tracing Configurations"* in *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide*.

  - Preupgrade consideration: When upgrading from 23.2.0 to 23.4.0, certain scenarios needs to be considered. For more information, see "*Preupgrade Tasks"* in *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide.*

- **Support for Non-SUPI based On Demand Discovery Caching of NF Profiles:** Policy supports caching the NF profiles at NRF Client received from non-SUPI based on-demand discovery from NRF. Caching the NF profiles avoids rediscovering the NF profiles from NRF for every new call flow related to AMF, SMF(Notification) and UDR. For more information, see "*Support for Non-SUPI based On Demand Discovery Caching of NF* Profiles" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.
- **Enhancements to discard policy for diameter sessions**: Discard policy for diameter sessions is enhanced with options to discard sessions based on priority and priority percentage. For more information, see "*Load Shedding Profiles"* section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.
- **Support for flexible billing day change**: Usage Monitoring on Gx interface supports changing the billing cycle of the active plan from monthly to yearly, weekly, daily, or hourly and the effect is based on the configured flexible billing day. For more information, see "Usage Monitoring on Gx interface" *section in Oracle Communications Cloud Native Core, Converged Policy User Guide.*
- **Pro-Rating of monthly quota**: Usage monitoring on Gx interface supports pro-rating of the quota volume when the billing cycle is changed. For more information, see "Usage Monitoring on Gx interface" *section in Oracle Communications Cloud Native Core, Converged Policy User Guide.*
- **Usage monitoring support at PCC rule level**: Policy supports Usage monitoring at either at PCC rule level or at session level. With this feature, usage monitoring can be requested on an individual rule (PCC rule level) or on all the rules activated during a IP-CAN session (session level). For more information, see "Usage Monitoring on Gx interface" *section in Oracle Communications Cloud Native Core, Converged Policy User Guide.*
- **Data Compression in Usage Monitoring**: In order to handle the growing size of the Usage Monitoring database and the replication volume, Policy supports compressing the Usage Monitoring data. For more information, see "Usage Monitoring on Gx interface" *section in Oracle Communications Cloud Native Core, Converged Policy User Guide.*
- **Migration of subscribers from OCPM to PCRF deployment**: Policy supports migrating the subscribers from OCPM deployment to CnPolicy deployment model. The migration includes the quota data as well as the dynamic quota data. For more information, see "*Migration of subscribers from OCPM to PCRF deployment"* section in *Oracle Communications Cloud Native Core, Converged Policy User Guide.*
- **Enhanced Policy Blockly support for UE Policy service conditions and actions**: New blocks are added to support UE Policy service conditions and actions. These new blocks enables to find the delta between the UPSI's id list and UPSI's currently configured in PCF, UPSI's that are sent on UE Policy registration and UPSI's that are on UDR. For more information on the enhancements see "Support for Listing and Comparing UPSIs Received from UDR" in *Oracle Communications Cloud Native Core, Converged Policy User Guide.* For details on the UE Policy blocks, actions, and conditions used for this functionality, see "*UE Policy"* section in *Oracle Communications Cloud Native Core, Converged Policy Design Guide*.
- **Support for Network Policies**: Network Policies are an application-centric construct that allows to specify how a pod communicates with various network entities. It creates pod-level rules to control communication between the cluster's pods and services, and to determine which pods and services can access one another inside a cluster. For more

information, see "*Network Policies*" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide.*

- **Handling Race Condition Between Gx and Sy Sessions over two sites**: Policy supports handling race condition between Gx and Sy sessions over two sites that result in Sy stale sessionsin PDS. For more information, see "*Handling Race Condition Between Gx and Sy Sessions over two sites"* section in *Oracle Communications Cloud Native Core, Converged Policy User Guide.*
- **Improvements to exception table maintenance**: Audit service is used to clean up exception tables for Binding service, AM service, SM service, UE Policy service, PCRF Core and PDS. The Audit service configuration for cleaning up these exception tables are predefined using Helm parameters at the time of installation with a default 24hr frequency for auditing. For more information, see "Audit Service" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide.*
- **ATS Feature Activation and Deactivation:** This feature allows to activate or deactivate the specific features within the ATS using Helm charts. Once these features are removed, they cannot be reinstated in the deployed ATS. However, users have the option to reinstall the ATS to restore the disabled features. For more information about the feature, see *"ATS Feature Activation and Deactivation"* section in *Oracle Communications Cloud Native Core, Automated Testing Suite Guide*.

## 2.12 Service Communication Proxy (SCP)

**Release 23.4.3**

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

**Release 23.4.2**

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

**Release 23.4.1**

Oracle Communications Cloud Native Core, Service Communication Proxy (SCP) 23.4.1 has been updated with the following enhancements:

- **NFProfile Processing Enhancements**: With this enhancement, whenever SCP receives a notification regarding an NF profile that includes 3GPP-defined supported NF services, custom, unknown, or unsupported NF services, SCP ignores the presence of custom, unknown, or unsupported NF services within the NF profile. Routing rules are generated by SCP for 3GPP-defined supported NF services that are present in the NF profile. Consequently, SCP enhanced the process of handling NF profiles by streamlining the routing process and ensuring efficient and reliable communication between NFs. For more information, see "NFProfile Processing Enhancements" in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.
- **Message Feed Enhancements**: SCP is enhanced to select Kafka partitions based on the `kafkaPartitionSelectionLogic` REST API configuration to distribute the messages to the same or different partitions in a Kafka broker. For more information, see "Message Feed Enhancements" in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.

**Release 23.4.0**

Oracle Communications Cloud Native Core, Service Communication Proxy (SCP) 23.4.0 has been updated with the following enhancements:

- **NRF Configuration Using DNS SRV Resolution**: Currently, SCP supports the static configuration (helm configuration) of NRF profiles from the custom-values.yaml file and uses them for registration, subscription, discovery, and audit. With the introduction of this feature, SCP supports the RESTful configuration of the NRF Service (SRV) FQDN at SCP. A user can configure primary (mandatory), secondary, and tertiary NRFs based on their priority and weights from different regions in the DNS server against an NRF SRV FQDN. For more information, see "NRF Configuration Using DNS SRV Resolution" in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.
- **Support for cnDBTier APIs in CNC Console**: With this enhancement, cnDBTier APIs are integrated into the CNC Console, and users can view specific cnDBTier statuses on the CNC Console. For more information, see "Support for cnDBTier APIs in CNC Console" in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.
- **SCP Response Timeout Extension**: SCP allows users to set a maximum response timeout of up to 15 seconds for all the services supported by the SCP for improved service reliability and responsiveness. For more information, see "SCP Response Timeout Extension" in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.
- **Custom Header Support at SCP**: With the introduction of this feature, efficiency is enhanced across the converged networks and optimized for 5G core traffic. For more information, see "Custom Header Support at SCP" in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.
- **Mediation Rule Configuration Enhancement**: This enhancement enables SCP to manage mediation rules in the database by retrieving, adding, and modifying them through the CNCC Console and Restful API. For more information, see "Mediation Rule Configuration Enhancement" in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.
- **Support for Automated Certificate Lifecycle Management**: This feature allows you to integrate SCP with Oracle Communications Cloud Native Core, Certificate Management (OCCM) to support automation of certificate lifecycle management. You can now monitor, create, recreate, and renew TLS certificates based on their validity. For more information, see "Support for Automated Certificate Lifecycle Management" in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide.*
- **Overload Control Based on the Overload Control Information (OCI) Header**: When SCP, SEPP, consumer NF, or producer NF is overloaded, it sends overload condition information through the 3gpp-Sbi-Oci header, which is tagged along with the messages, to peer NFs. For more information, see "Overload Control Based on the Overload Control Information Header" in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide.*
- **Load Balancing Support for Delegated Discovery**: This enhancement allows user to change the preferred NRF instance ID or NRF Set ID for delegated discovery at runtime using the REST API. For more information, see "Support for Model D Indirect 5G SBI Communication with Delegated Discovery" in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.

## 2.13 Security Edge Protection Proxy (SEPP)

**Release 23.4.2**

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

### Release 23.4.1

SEPP 23.4.1 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 23.4.0

Oracle Communications Cloud Native Core, Security Edge Protection Proxy (SEPP) 23.4.0 has been updated with the following enhancements:

- **Load Sharing among Multiple Remote SEPP Nodes**: With load sharing among multiple Remote SEPP nodes feature, SEPP can now efficiently distribute incoming traffic among multiple remote SEPPs. To enable this, the operator needs to configure a single virtual FQDN for the remote SEPPs. SEPP retrieves multiple Remote SEPP records from the DNS server and distributes the traffic according to the priority and weight associated with each record. Hence, SEPP can simultaneously route the incoming requests to multiple Remote SEPPs. For more information about the feature, see the *"Load Sharing among Multiple Remote SEPP Nodes"* section in *Oracle Communications Cloud Native Core, Security Edge Protection Proxy User Guide* and the *"Remote SEPP"* section in *Oracle Communications Cloud Native Core, Security Edge Protection Proxy REST API Specification Guide*.
- **Separate Port Configurations for N32c and N32f on the Egress Routes**: In some deployments, there is a need to have different service IPs and ports for n32c and n32f interfaces although the endpoint SEPP may have the same name. To improve traffic segregation, the Egress Gateway is enhanced by configuring different ports for the n32c and n32f connections on both the Remote SEPP Set and its local configurations. Separate ports for n32c and n32f interfaces provide the flexibility to configure different IP addresses or ports for both interfaces. For more information about the feature, see the *"Separate Port Configurations for N32c and N32f on the Egress Routes"* section in *Oracle Communications Cloud Native Core, Security Edge Protection Proxy User Guide* and the *"Remote SEPP"* section in *Oracle Communications Cloud Native Core, Security Edge Protection Proxy REST API Specification Guide*.
- **Support for cnDBTier APIs in CNC Console**: With the implementation of this feature, cnDBTier APIs are integrated into the CNC Console. SEPP users can view specific cnDBTier APIs such as checking the cnDBTier version, status of cnDBTier clusters, and georeplication status on the CNC Console. The cnDBTier APIs can be viewed (read-only) from 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*.
- **Mediation Rules using CNC Console and REST APIs**: With this feature enhancement, mediation rules are being stored in the database. The existing rules can be retrieved, modified, deleted, and new rules can be configured and applied to mediation microservice using the CNC Console or REST APIs. For more information about the feature, see the *"5G SBI Message Mediation Support"* section in *Oracle Communications Cloud Native Core, Security Edge Protection Proxy User Guide* and the *"Mediation Rules Configuration"* section in *Oracle Communications Cloud Native Core, Security Edge Protection Proxy REST API Specification Guide*.
- **ATS Feature Activation and Deactivation**: This feature allows to activate or deactivate the specific features within the ATS using Helm charts. Once these features are removed, they cannot be reinstated in the deployed ATS. However, users have the option to reinstall

the ATS to restore the disabled features. For more information about the feature, see *"ATS Feature Activation and Deactivation"* section in *Oracle Communications Cloud Native Core, Automated Testing Suite Guide*.

- **Support for Transport Layer Security in ATS**: With the support of the TLS feature, Jenkins servers have been upgraded to support HTTPS, ensuring a secure and encrypted connection when accessing the ATS dashboard. To provide encryption, HTTPS uses an encryption protocol known as Transport Layer Security (TLS), which is a widely accepted standard protocol that provides authentication, privacy, and data integrity between two communicating computer applications. For more information about the feature, see *"Support for Transport Layer Security"* and *"Installing SEPP"* sections in *Oracle Communications Cloud Native Core, Automated Testing Suite Guide*.
- **Individual Stage Group Selection**: This feature allows users to select and run single or multiple stages or groups by selecting a check box for the corresponding stage or group. For more information, see *"Individual Stage Group Selection"* in *Oracle Communications Cloud Native Core, Automated Test Suite Guide*.

# 2.14 Unified Data Repository (UDR)

**Release 23.4.2**

Oracle Communications Cloud Native Core, Unified Data Repository (UDR) 23.4.2 has been updated with the following enhancements:

- **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 header 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.*

**Release 23.4.1**

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

**Release 23.4.0**

Oracle Communications Cloud Native Core, Unified Data Repository (UDR) 23.4.0 has been updated with the following enhancements:

- **Migration Tool Support for Converged Quota**: The migration tool is enhanced to support converged quota and it also supports monitoring and pausing the migration tool using REST API and CNC Console. For more information about the feature, see *"Converged Quota Support for UDR"* section in *Oracle Communications Cloud Native Core, Unified Data Repository User Guide*.
- **Support for EXML Format**: This feature allows to export the subscriber data in EXML format, which is compatible with 4G OCUDR export format. It supports the export of 4G policy data (VSA and umData/umDataLimits) in EXML format from 5G UDR to 4G OCUDR using the subscriber export tool. For more information about the feature, see *"Support for EXML Format"* section in *Oracle Communications Cloud Native Core, Unified Data Repository User Guide*.
- **User Equipment Optimization support for Equipment Identity Register (EIR)**: As per 3GPP standards, all User Equipment (UE) in the operator's network is declared within the EIR database as Whitelisted, Greylisted, or Blacklisted. The UEs that are not declared in

the EIR database are categorized Blacklisted by default. As all UE Permanent Equipment Identifier (PEI) and International Mobile Equipment Identity (IMEI) cannot be provisioned in EIR database, this feature allows the operators to configure a default response for unknown UE. For more information about the feature, see *"User Equipment Optimization support in EIR"* section in *Oracle Communications Cloud Native Core, Unified Data Repository User Guide*.

- **Provisioning Gateway Network Layout Changes**: This feature enhances the provisioning system to support the provisioning in active-active mode. Each provisioning system instance has its own preferred Provisioning Gateway to ensure that the traffic is distributed to all the Provisioning Gateway instances. For more information about the feature, see *"Provisioning Gateway Network Layout Changes"* section in *Oracle Communications Cloud Native Core, Provisioning Gateway Guide*.
- **Support for cnDBTier APIs in CNC Console**: UDR supports to view certain cnDBTier APIs from CNC Console when the cnDBTier APIs are integrated into the CNC Console. For more information about integration of cnDBTier APIs in CNC Console, see *"Support for cnDBTier APIs in CNC Console"* in *Oracle Communications Cloud Native Core, Unified Data Repository User Guide*.
- **ATS Parallel Test Execution:** This feature allows you to perform multiple logically grouped ATS tests simultaneously on the same System Under Test (SUT) to reduce the overall execution time of ATS. For more information about the feature, see *"Parallel Test Execution"* section in *Oracle Communications Cloud Native Core, Automated Testing Suite Guide*.

# 3 Media and Documentation

## 3.1 Media Pack

This section lists the media package for Oracle Communications Cloud Native Core 3.23.4. To download the media package, see MOS.

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

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

**Table 3-1 Media Pack Contents for Oracle Communications Cloud Native Core 3.23.4**

| Description | NF Version | ATS Version | Upgrade Supported |
|---|---|---|---|
| Oracle Communications Cloud Native Core, Binding Support Function (BSF) | 23.4.4 | 23.4.4 | BSF 23.4.4 supports fresh installation and upgrade from 23.4.x and 23.2.x. For more information, see *Oracle Communications Cloud Native Core, Binding Support Function Installation, Upgrade, and Fault Recovery Guide*. |
| Oracle Communications Cloud Native Core, Binding Support Function (BSF) | 23.4.2 | 23.4.2 | BSF 23.4.2 supports fresh installation and upgrade from 23.4.x and 23.2.x. For more information, see *Oracle Communications Cloud Native Core, Binding Support Function Installation, Upgrade, and Fault Recovery Guide*. |
| Oracle Communications Cloud Native Core, Binding Support Function (BSF) | 23.4.1 | 23.4.1 | BSF 23.4.1 supports fresh installation and upgrade from 23.4.0 and 23.2.x. For more information, see *Oracle Communications Cloud Native Core, Binding Support Function Installation, Upgrade, and Fault Recovery Guide*. |
| Oracle Communications Cloud Native Core, Binding Support Function (BSF) | 23.4.0 | 23.4.0 | BSF 23.4.0 supports fresh installation and upgrade from 23.2.x. For more information, see *Oracle Communications Cloud Native Core, Binding Support Function Installation, Upgrade, and Fault Recovery Guide*. |

**Table 3-1 (Cont.) Media Pack Contents for Oracle Communications Cloud Native Core 3.23.4**

| Description | NF Version | ATS Version | Upgrade Supported |
|---|---|---|---|
| Oracle Communications Cloud Native Configuration Console (CNC Console) | 23.4.2 | NA | CNC Console 23.4.2 supports fresh installation and upgrade from 23.3.x and 23.4.x. For more information, see *Oracle Communications Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide*. |
| Oracle Communications Cloud Native Configuration Console (CNC Console) | 23.4.1 | NA | CNC Console 23.4.1 supports fresh installation and upgrade from 23.2.x, 23.3.x, and 23.4.0. For more information, see *Oracle Communications Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide*. |
| Oracle Communications Cloud Native Configuration Console (CNC Console) | 23.4.0 | NA | CNC Console 23.4.0 supports fresh installation and upgrade from 23.2.x and 23.3x. For more information, see *Oracle Communications Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide*. |
| Oracle Communications Cloud Native Core, Certificate Management (OCCM) | 23.4.3 | NA | OCCM 23.4.3 supports fresh installation and upgrade from 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) | 23.4.2 | NA | OCCM 23.4.2 supports fresh installation and upgrade from 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) | 23.4.1 | NA | OCCM 23.4.1 supports fresh installation and upgrade from 23.4.0. 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) | 23.4.0 | NA | OCCM 23.4.0 supports fresh installation. 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 3.23.4

| Description | NF Version | ATS Version | Upgrade Supported |
|---|---|---|---|
| Oracle Communications Cloud Native Core, cnDBTier | 23.4.6 | NA | cnDBTier 23.4.6 supports fresh installation and upgrade from 23.2.x, 23.3.x, and 23.4.x. For more information, see *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*.<br>**Note**: cnDBTier 23.4.6 doesn't support upgrade and rollback on cnDBTier setups where the TLS feature is enabled. |
| Oracle Communications Cloud Native Core, cnDBTier | 23.4.5 | NA | cnDBTier 23.4.5 supports fresh installation and upgrade from 23.2.x, 23.3.x, and 23.4.x. For more information, see *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*.<br>**Note**: cnDBTier 23.4.5 doesn't support upgrade and rollback on cnDBTier setups where the TLS feature is enabled. |
| Oracle Communications Cloud Native Core, cnDBTier | 23.4.4 | NA | cnDBTier 23.4.4 supports fresh installation and upgrade from 23.2.x, 23.3.x, and 23.4.x. For more information, see *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*.<br>**Note**: cnDBTier 23.4.4 doesn't support upgrade and rollback on cnDBTier setups where the TLS feature is enabled. |
| Oracle Communications Cloud Native Core, cnDBTier | 23.4.3 | NA | cnDBTier 23.4.3 supports fresh installation and upgrade from 23.2.x, 23.3.x, and 23.4.x. For more information, see *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*.<br>**Note**: cnDBTier 23.4.3 doesn't support upgrade and rollback on cnDBTier setups where the TLS feature is enabled. |

**Table 3-1 (Cont.) Media Pack Contents for Oracle Communications Cloud Native Core 3.23.4**

| Description | NF Version | ATS Version | Upgrade Supported |
|---|---|---|---|
| Oracle Communications Cloud Native Core, cnDBTier | 23.4.2 | NA | cnDBTier 23.4.2 supports fresh installation and upgrade from 23.2.x, 23.3.x, and 23.4.x. For more information, see *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*.<br>**Note**: cnDBTier 23.4.2 doesn't support upgrade and rollback on cnDBTier setups where the TLS feature is enabled. |
| Oracle Communications Cloud Native Core, cnDBTier | 23.4.1 | NA | cnDBTier 23.4.1 supports fresh installation and upgrade from 23.2.x, 23.3.x, and 23.4.0. For more information, see *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*.<br>**Note**: cnDBTier 23.4.1 doesn't support upgrade and rollback on cnDBTier setups where the TLS feature is enabled. |
| Oracle Communications Cloud Native Core, cnDBTier | 23.4.0 | NA | cnDBTier 23.4.0 supports fresh installation and upgrade from 23.2.x and 23.3.x. For more information, see *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*.<br>**Note**: cnDBTier 23.4.0 doesn't support upgrade and rollback on cnDBTier setups where the TLS feature is enabled. |
| Oracle Communications CD Control Server (CDCS) | 23.4.0 | NA | CDCS 23.4.0 supports only fresh installation. For more information, see *Oracle Communications CD Control Server Installation and Upgrade Guide.* |
| Oracle Communications Cloud Native Core, Cloud Native Environment (CNE) | 23.4.6 | NA | CNE 23.4.6 supports fresh installation and upgrade from 23.3.x and 23.4.x. For more information, see *Oracle Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide.* |
| Oracle Communications Cloud Native Core, Cloud Native Environment (CNE) | 23.4.4 | NA | CNE 23.4.4 supports fresh installation and upgrade from 23.3.x and 23.4.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 3.23.4

| Description | NF Version | ATS Version | Upgrade Supported |
|---|---|---|---|
| Oracle Communications Cloud Native Core, Cloud Native Environment (CNE) | 23.4.1 | NA | CNE 23.4.1 supports fresh installation and upgrade from 23.3.x and 23.4.0. For more information, see *Oracle Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide.* |
| Oracle Communications Cloud Native Core, Cloud Native Environment (CNE) | 23.4.0 | NA | CNE 23.4.0 supports only fresh installation. For more information, see *Oracle Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide.* |
| Oracle Communications Operations Services Overlay (OSO) | 23.4.5 | NA | OSO 23.4.5 supports fresh installation and upgrade from 23.3.1 and 23.4.x. For more information, see *Oracle Communications Operations Services Overlay Installation and Upgrade Guide*. |
| Oracle Communications Operations Services Overlay (OSO) | 23.4.4 | NA | OSO 23.4.4 supports fresh installation and upgrade from 23.3.1 and 23.4.0. For more information, see *Oracle Communications Operations Services Overlay Installation and Upgrade Guide*. |
| Oracle Communications Operations Services Overlay (OSO) | 23.4.0 | NA | OSO 23.4.0 supports fresh installation and upgrade from 23.3.1. For more information, see *Oracle Communications Operations Services Overlay Installation and Upgrade Guide*. |
| Oracle Communications Cloud Native Core, Network Exposure Function (NEF) | 23.4.4 | 23.4.4 | NEF 23.4.4 supports fresh installation and upgrade from 23.2.x, 23.3.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 Exposure Function (NEF) | 23.4.3 | 23.4.3 | NEF 23.4.3 supports fresh installation and upgrade from 23.2.x, 23.3.x, and 23.4.x. For more information, see *Oracle Communications Cloud Native Core, Network Exposure Function Installation, Upgrade, and Fault Recovery Guide*. |

Table 3-1 (Cont.) Media Pack Contents for Oracle Communications Cloud Native Core 3.23.4

| Description | NF Version | ATS Version | Upgrade Supported |
|---|---|---|---|
| Oracle Communications Cloud Native Core, Network Exposure Function (NEF) | 23.4.2 | 23.4.0 | NEF 23.4.2 supports fresh installation and upgrade from 23.2.x, 23.3.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 Exposure Function (NEF) | 23.4.1 | 23.4.0 | NEF 23.4.1 supports fresh installation and upgrade from 23.2.x, 23.3.x, and 23.4.0. For more information, see *Oracle Communications Cloud Native Core, Network Exposure Function Installation, Upgrade, and Fault Recovery Guide*. |
| Oracle Communications Cloud Native Core, Network Exposure Function (NEF) | 23.4.0 | 23.4.0 | NEF 23.4.0 supports fresh installation and upgrade from 23.2.x and 23.3.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) | 23.4.4 | 23.4.4 | NRF 23.4.4 supports fresh installation and upgrade from 23.3.x and 23.4.x. For more information, see *Oracle Communications Cloud Native Core, Network Repository Function Installation, Upgrade, and Fault Recovery Guide*. |
| Oracle Communications Cloud Native Core, Network Repository Function (NRF) | 23.4.3 | 23.4.4 | NRF 23.4.3 supports fresh installation and upgrade from 23.3.x and 23.4.x. For more information, see *Oracle Communications Cloud Native Core, Network Repository Function Installation, Upgrade, and Fault Recovery Guide*. |
| Oracle Communications Cloud Native Core, Network Repository Function (NRF) | 23.4.2 | 23.4.3 | NRF 23.4.2 supports fresh installation and upgrade from 23.3.x and 23.4.x. For more information, see *Oracle Communications Cloud Native Core, Network Repository Function Installation, Upgrade, and Fault Recovery Guide*. |
| Oracle Communications Cloud Native Core, Network Repository Function (NRF) | 23.4.1 | 23.4.2 | NRF 23.4.1 supports fresh installation and upgrade from 23.3.x and 23.4.0. 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 3.23.4**

| Description | NF Version | ATS Version | Upgrade Supported |
|---|---|---|---|
| Oracle Communications Cloud Native Core, Network Repository Function (NRF) | 23.4.0 | 23.4.0, 23.4.1 | NRF 23.4.0 supports fresh installation and upgrade from 23.3.x. For more information, see *Oracle Communications Cloud Native Core, Network Repository Function Installation, Upgrade, and Fault Recovery Guide*. |
| Oracle Communications Cloud Native Core, Network Slice Selection Function (NSSF) | 23.4.0 | 23.4.0 | NSSF 23.4.0 supports fresh installation and upgrade from 23.3.x. For more information, see *Oracle Communications Cloud Native Core, Network Slice Selection Function Installation, Upgrade, and Fault Recovery Guide*.<br>**Note**: In a georedundant scenario, the replication channel may go down while doing a rollback of cnDBTier from 23.4.x to 23.3.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, Converged Policy (Policy) | 23.4.6 | 23.4.5 | Policy 23.4.6 supports fresh installation and upgrade from 23.4.x and 23.2.x. For more information, see *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide*. |
| Oracle Communications Cloud Native Core, Converged Policy (Policy) | 23.4.5 | 23.4.5 | Policy 23.4.5 supports fresh installation and upgrade from 23.4.x and 23.2.x. For more information, see *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide*. |
| Oracle Communications Cloud Native Core, Converged Policy (Policy) | 23.4.4 | 23.4.2 | Policy 23.4.4 supports fresh installation and upgrade from 23.4.x and 23.2.x. For more information, see *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide*. |
| Oracle Communications Cloud Native Core, Converged Policy (Policy) | 23.4.3 | 23.4.2 | Policy 23.4.3 supports fresh installation and upgrade from 23.4.x and 23.2.x. For more information, see *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide*. |

Table 3-1 (Cont.) Media Pack Contents for Oracle Communications Cloud Native Core 3.23.4

| Description | NF Version | ATS Version | Upgrade Supported |
|---|---|---|---|
| Oracle Communications Cloud Native Core, Converged Policy (Policy) | 23.4.2 | 23.4.1 | Policy 23.4.2 supports fresh installation and upgrade from 23.4.x and 23.2.x. For more information, see *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide*. |
| Oracle Communications Cloud Native Core, Converged Policy (Policy) | 23.4.1 | 23.4.1 | Policy 23.4.1 supports fresh installation and upgrade from 23.4.0 and 23.2.x. For more information, see *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide*. |
| Oracle Communications Cloud Native Core, Converged Policy (Policy) | 23.4.0 | 23.4.0 | Policy 23.4.0 supports fresh installation and upgrade from 23.2.x. For more information, see *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide*. |
| Oracle Communications Cloud Native Core, Service Communications Proxy (SCP) | 23.4.3 | 23.4.3 | SCP 23.4.3 supports fresh installation and upgrade from 23.2.x, 23.3.x, and 23.4.x. For more information, see *Oracle Communications Cloud Native Core, Service Communication Proxy Installation, Upgrade, and Fault Recovery Guide*. |
| Oracle Communications Cloud Native Core, Service Communications Proxy (SCP) | 23.4.2 | 23.4.2 | SCP 23.4.2 supports fresh installation and upgrade from 23.2.x, 23.3.x, and 23.4.x. For more information, see *Oracle Communications Cloud Native Core, Service Communication Proxy Installation, Upgrade, and Fault Recovery Guide*. |
| Oracle Communications Cloud Native Core, Service Communications Proxy (SCP) | 23.4.1 | 23.4.1 | SCP 23.4.1 supports fresh installation and upgrade from 23.2.x, 23.3.x, and 23.4.x. For more information, see *Oracle Communications Cloud Native Core, Service Communication Proxy Installation, Upgrade, and Fault Recovery Guide*. |
| Oracle Communications Cloud Native Core, Service Communications Proxy (SCP) | 23.4.0 | 23.4.0 | SCP 23.4.0 supports fresh installation and upgrade from 23.2.x and 23.3.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 3.23.4**

| Description | NF Version | ATS Version | Upgrade Supported |
|---|---|---|---|
| Oracle Communications Cloud Native Core, Security Edge Protection Proxy (SEPP) | 23.4.2 | 23.4.2 | SEPP 23.4.2 supports fresh installation and upgrade from 23.2.x, 23.3.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) | 23.4.1 | 23.4.1 | SEPP 23.4.1 supports fresh installation and upgrade from 23.4.0, 23.2.x, and 23.3.x. For more information, see *Oracle Communications Cloud Native Core, Security Edge Protection Proxy Installation, Upgrade, and Fault Recovery Guide.* |
| Oracle Communications Cloud Native Core, Security Edge Protection Proxy (SEPP) | 23.4.0 | 23.4.0 | SEPP 23.4.0 supports fresh installation and upgrade from 23.2.x and 23.3.x. For more information, see *Oracle Communications Cloud Native Core, Security Edge Protection Proxy Installation, Upgrade, and Fault Recovery Guide.* |
| Oracle Communications Cloud Native Core, Unified Data Repository (UDR) | 23.4.2 | 23.4.4 | UDR 23.4.2 supports fresh installation and upgrade from 23.2.x, 23.3.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) | 23.4.1 | 23.4.0, 23.4.1, 23.4.2, and 23.4.3 | UDR 23.4.1 supports fresh installation and upgrade from 23.2.x, 23.3.x, and 23.4.0. For more information, see *Oracle Communications Cloud Native Core, Unified Data Repository Installation, Upgrade, and Fault Recovery Guide*. |
| Oracle Communications Cloud Native Core, Unified Data Repository (UDR) | 23.4.0 | 23.4.0, 23.4.1, and 23.4.2 | UDR 23.4.0 supports fresh installation and upgrade from 23.2.x and 23.3.x. For more information, see *Oracle Communications Cloud Native Core, Unified Data Repository Installation, Upgrade, and Fault Recovery Guide*. |

## 3.2 Compatibility Matrix

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

**Table 3-2 Compatibility Matrix**

| CNC NF | NF Version | CNE | cnDBTier | CDCS | OSO | ASM S/W | Kubernetes | CNC Console | OCNADD | OCCM |
|---|---|---|---|---|---|---|---|---|---|---|
| **BSF** | 23.4.4 | • 23.4.x<br>• 23.2.x | • 23.4.x<br>• 23.2.x | NA | • 23.4.x<br>• 23.2.x | 1.14.6 | • 1.27.x<br>• 1.25.x | • 23.4.x<br>• 23.2.x | NA | NA |
| **BSF** | 23.4.2 | • 23.4.x<br>• 23.2.x | • 23.4.x<br>• 23.2.x | NA | • 23.4.x<br>• 23.2.x | 1.14.6 | • 1.27.x<br>• 1.25.x | • 23.4.x<br>• 23.2.x | NA | NA |
| **BSF** | 23.4.1 | • 23.4.x<br>• 23.2.x | • 23.4.x<br>• 23.2.x | NA | • 23.4.x<br>• 23.2.x | 1.14.6 | • 1.27.x<br>• 1.25.x | • 23.4.x<br>• 23.2.x | NA | NA |
| **BSF** | 23.4.0 | • 23.4.x<br>• 23.2.x | • 23.4.x<br>• 23.2.x | NA | • 23.4.x<br>• 23.2.x | 1.14.6 | • 1.27.x<br>• 1.25.x | • 23.4.x<br>• 23.2.x | NA | NA |
| **CDCS** | 23.4.0 | • 23.4.x<br>• 23.3.x<br>• 23.2.x<br>• 23.1.x | NA | NA | NA | NA | NA | NA | NA | NA |
| **CNC Console** | 23.4.2 | • 23.4.x<br>• 23.3.x<br>• 23.2.x | • 23.4.x<br>• 23.3.x<br>• 23.2.x | • 23.4.x<br>• 23.3.x<br>• 23.2.x | • 23.4.x<br>• 23.3.x<br>• 23.2.x | • 1.14.6<br>• 1.11.8<br>• 1.9.8 | • 1.27.x<br>• 1.26.x<br>• 1.25.x | NA | 23.4.x | 23.4.x |
| **CNC Console** | 23.4.1 | • 23.4.x<br>• 23.3.x<br>• 23.2.x | • 23.4.x<br>• 23.3.x<br>• 23.2.x | • 23.4.x<br>• 23.3.x<br>• 23.2.x | • 23.4.x<br>• 23.3.x<br>• 23.2.x | • 1.14.6<br>• 1.11.8<br>• 1.9.8 | • 1.27.x<br>• 1.26.x<br>• 1.25.x | NA | 23.4.x | 23.4.x |
| **CNC Console** | 23.4.0 | • 23.4.x<br>• 23.3.x<br>• 23.2.x | • 23.4.x<br>• 23.3.x<br>• 23.2.x | • 23.4.x<br>• 23.3.x<br>• 23.2.x | • 23.4.x<br>• 23.3.x<br>• 23.2.x | • 1.14.6<br>• 1.11.8<br>• 1.9.8 | • 1.27.x<br>• 1.26.x<br>• 1.25.x | NA | 23.4.x | 23.4.x |
| **cnDBTier** | 23.4.6 | • 23.4.x<br>• 23.3.x<br>• 23.2.x | NA | 23.4.x | NA | NA | • 1.27.x<br>• 1.26.x<br>• 1.25.x | NA | NA | NA |
| **cnDBTier** | 23.4.5 | • 23.4.x<br>• 23.3.x<br>• 23.2.x | NA | 23.4.x | NA | NA | • 1.27.x<br>• 1.26.x<br>• 1.25.x | NA | NA | NA |
| **cnDBTier** | 23.4.4 | • 23.4.x<br>• 23.3.x<br>• 23.2.x | NA | 23.4.x | NA | NA | • 1.27.x<br>• 1.26.x<br>• 1.25.x | NA | NA | NA |

**Table 3-2 (Cont.) Compatibility Matrix**

| CNC NF | NF Version | CNE | cnDBTier | CDCS | OSO | ASM S/W | Kubernetes | CNC Console | OCNADD | OCCM |
|---|---|---|---|---|---|---|---|---|---|---|
| **cnDBTier** | 23.4.3 | • 23.4.x<br>• 23.3.x<br>• 23.2.x | NA | 23.4.x | NA | NA | • 1.27.x<br>• 1.26.x<br>• 1.25.x | NA | NA | NA |
| **cnDBTier** | 23.4.2 | • 23.4.x<br>• 23.3.x<br>• 23.2.x | NA | 23.4.x | NA | NA | • 1.27.x<br>• 1.26.x<br>• 1.25.x | NA | NA | NA |
| **cnDBTier** | 23.4.1 | • 23.4.x<br>• 23.3.x<br>• 23.2.x | NA | 23.4.x | NA | NA | • 1.27.x<br>• 1.26.x<br>• 1.25.x | NA | NA | NA |
| **cnDBTier** | 23.4.0 | • 23.4.x<br>• 23.3.x<br>• 23.2.x | NA | 23.4.x | NA | NA | • 1.27.x<br>• 1.26.x<br>• 1.25.x | NA | NA | NA |
| **CNE** | 23.4.6 | NA | NA | NA | NA | NA | 1.27.x | NA | NA | NA |
| **CNE** | 23.4.4 | NA | NA | NA | NA | NA | 1.27.x | NA | NA | NA |
| **CNE** | 23.4.1 | NA | NA | NA | NA | NA | 1.27.x | NA | NA | NA |
| **CNE** | 23.4.0 | NA | NA | NA | NA | NA | 1.27.x | NA | NA | NA |
| **OCCM** | 23.4.3 | • 23.4.x<br>• 23.3.x<br>• 23.2.x | NA | • 23.4.x<br>• 23.3.x | NA | NA | • 1.27.x<br>• 1.26.x<br>• 1.25.x | 23.4.x | NA | NA |
| **OCCM** | 23.4.2 | • 23.4.x<br>• 23.3.x<br>• 23.2.x | NA | • 23.4.x<br>• 23.3.x | NA | NA | • 1.27.x<br>• 1.26.x<br>• 1.25.x | 23.4.x | NA | NA |
| **OCCM** | 23.4.1 | • 23.4.x<br>• 23.3.x<br>• 23.2.x | NA | • 23.4.x<br>• 23.3.x | NA | NA | • 1.27.x<br>• 1.26.x<br>• 1.25.x | 23.4.x | NA | NA |
| **OCCM** | 23.4.0 | • 23.4.x<br>• 23.3.x<br>• 23.2.x | NA | • 23.4.x<br>• 23.3.x | NA | NA | • 1.27.x<br>• 1.26.x<br>• 1.25.x | 23.4.x | NA | NA |
| **OSO** | 23.4.5 | NA | NA | NA | NA | NA | • 1.27.x<br>• 1.26.x | NA | NA | NA |
| **OSO** | 23.4.4 | NA | NA | NA | NA | NA | • 1.27.x<br>• 1.26.x | NA | NA | NA |
| **OSO** | 23.4.0 | NA | NA | NA | NA | NA | • 1.27.x<br>• 1.26.x | NA | NA | NA |
| **NEF** | 23.4.4 | • 23.4.x<br>• 23.3.x<br>• 23.2.x | • 23.4.x<br>• 23.3.x<br>• 23.2.x | NA | NA | NA | • 1.27.x<br>• 1.26.x<br>• 1.25.x | NA | NA | NA |
| **NEF** | 23.4.3 | • 23.4.x<br>• 23.3.x<br>• 23.2.x | • 23.4.x<br>• 23.3.x<br>• 23.2.x | NA | NA | NA | • 1.27.x<br>• 1.26.x<br>• 1.25.x | NA | NA | NA |

Table 3-2 (Cont.) Compatibility Matrix

| CNC NF | NF Version | CNE | cnDBTier | CDCS | OSO | ASM S/W | Kubernetes | CNC Console | OCNADD | OCCM |
|---|---|---|---|---|---|---|---|---|---|---|
| **NEF** | 23.4.2 | 23.4.x<br>23.3.x<br>23.2.x | 23.4.x<br>23.3.x<br>23.2.x | NA | NA | NA | 1.27.x<br>1.26.x<br>1.25.x | NA | NA | NA |
| **NEF** | 23.4.1 | 23.4.x<br>23.3.x<br>23.2.x | 23.4.x<br>23.3.x<br>23.2.x | NA | NA | NA | 1.27.x<br>1.26.x<br>1.25.x | NA | NA | NA |
| **NEF** | 23.4.0 | 23.4.x<br>23.3.x<br>23.2.x | 23.4.x<br>23.3.x<br>23.2.x | NA | NA | NA | 1.27.x<br>1.26.x<br>1.25.x | NA | NA | NA |
| **NRF** | 23.4.4 | 23.4.x<br>23.3.x<br>23.2.x | 23.4.x<br>23.3.x<br>23.2.x | 23.4.x<br>23.3.x<br>23.2.x | 23.4.x | 1.14.6 | 1.27.x<br>1.26.x<br>1.25.x | 23.4.x | 23.4.x | 23.4.x |
| **NRF** | 23.4.3 | 23.4.x<br>23.3.x<br>23.2.x | 23.4.x<br>23.3.x<br>23.2.x | 23.4.x<br>23.3.x<br>23.2.x | 23.4.x | 1.14.6 | 1.27.x<br>1.26.x<br>1.25.x | 23.4.x | 23.4.x | 23.4.x |
| **NRF** | 23.4.2 | 23.4.x<br>23.3.x<br>23.2.x | 23.4.x<br>23.3.x<br>23.2.x | 23.4.x<br>23.3.x<br>23.2.x | 23.4.x | 1.14.6 | 1.27.x<br>1.26.x<br>1.25.x | 23.4.x | 23.4.x | 23.4.x |
| **NRF** | 23.4.1 | 23.4.x<br>23.3.x<br>23.2.x | 23.4.x<br>23.3.x<br>23.2.x | 23.4.x<br>23.3.x<br>23.2.x | 23.4.x | 1.14.6 | 1.27.x<br>1.26.x<br>1.25.x | 23.4.x | 23.4.x | 23.4.x |
| **NRF** | 23.4.0 | 23.4.x<br>23.3.x<br>23.2.x | 23.4.x<br>23.3.x<br>23.2.x | 23.4.x<br>23.3.x<br>23.2.x | 23.4.x | 1.14.6 | 1.27.x<br>1.26.x<br>1.25.x | 23.4.x | 23.4.x | 23.4.x |
| **NSSF** | 23.4.0 | 23.4.x<br>23.3.x<br>23.2.x | 23.4.x<br>23.3.x<br>23.2.x | 23.4.x<br>23.3.x<br>23.2.x | 23.4.x | 1.14.6 | 1.27.x<br>1.26.x<br>1.25.x | 23.4.x | 23.4.x | 23.4.x |
| **Policy** | 23.4.6 | 23.4.x<br>23.2.x | 23.4.x<br>23.2.x | NA | 23.4.x | 1.14.6 | 1.27.x<br>1.25.x | 23.4.x<br>23.2.x | NA | NA |
| **Policy** | 23.4.5 | 23.4.x<br>23.2.x | 23.4.x<br>23.2.x | NA | 23.4.x | 1.14.6 | 1.27.x<br>1.25.x | 23.4.x<br>23.2.x | NA | NA |

**Table 3-2 (Cont.) Compatibility Matrix**

| CNC NF | NF Version | CNE | cnDBTier | CDCS | OSO | ASM S/W | Kubernetes | CNC Console | OCNADD | OCCM |
|---|---|---|---|---|---|---|---|---|---|---|
| **Policy** | 23.4.4 | • 23.4.x<br>• 23.2.x | • 23.4.x<br>• 23.2.x | NA | • 23.4.x<br>• 23.2.x | 1.14.6 | • 1.27.x<br>• 1.25.x | • 23.4.x<br>• 23.2.x | NA | NA |
| **Policy** | 23.4.3 | • 23.4.x<br>• 23.2.x | • 23.4.x<br>• 23.2.x | NA | • 23.4.x<br>• 23.2.x | 1.14.6 | • 1.27.x<br>• 1.25.x | • 23.4.x<br>• 23.2.x | NA | NA |
| **Policy** | 23.4.2 | • 23.4.x<br>• 23.2.x | • 23.4.x<br>• 23.2.x | NA | • 23.4.x<br>• 23.2.x | 1.14.6 | • 1.27.x<br>• 1.25.x | • 23.4.x<br>• 23.2.x | NA | NA |
| **Policy** | 23.4.1 | • 23.4.x<br>• 23.2.x | • 23.4.x<br>• 23.2.x | NA | • 23.4.x<br>• 23.2.x | 1.14.6 | • 1.27.x<br>• 1.25.x | • 23.4.x<br>• 23.2.x | NA | NA |
| **Policy** | 23.4.0 | • 23.4.x<br>• 23.2.x | • 23.4.x<br>• 23.2.x | NA | • 23.4.x<br>• 23.2.x | 1.14.6 | • 1.27.x<br>• 1.25.x | • 23.4.x<br>• 23.2.x | NA | NA |
| **SCP** | 23.4.3 | • 23.4.x<br>• 23.3.x<br>• 23.2.x | • 23.4.x<br>• 23.3.x<br>• 23.2.x | • 23.4.x<br>• 23.3.x<br>• 23.2.x | • 23.4.x<br>• 23.3.x<br>• 23.2.x | • 1.14.6<br>• 1.11.8 | • 1.27.x<br>• 1.26.x<br>• 1.25.x | 23.4.x | 23.4.x | 23.4.x |
| **SCP** | 23.4.2 | • 23.4.x<br>• 23.3.x<br>• 23.2.x | • 23.4.x<br>• 23.3.x<br>• 23.2.x | • 23.4.x<br>• 23.3.x<br>• 23.2.x | • 23.4.x<br>• 23.3.x<br>• 23.2.x | • 1.14.6<br>• 1.11.8 | • 1.27.x<br>• 1.26.x<br>• 1.25.x | 23.4.x | 23.4.x | 23.4.x |
| **SCP** | 23.4.1 | • 23.4.x<br>• 23.3.x<br>• 23.2.x | • 23.4.x<br>• 23.3.x<br>• 23.2.x | • 23.4.x<br>• 23.3.x<br>• 23.2.x | • 23.4.x<br>• 23.3.x<br>• 23.2.x | • 1.14.6<br>• 1.11.8 | • 1.27.x<br>• 1.26.x<br>• 1.25.x | 23.4.x | 23.4.x | 23.4.x |
| **SCP** | 23.4.0 | • 23.4.x<br>• 23.3.x<br>• 23.2.x | • 23.4.x<br>• 23.3.x<br>• 23.2.x | • 23.4.x<br>• 23.3.x<br>• 23.2.x | • 23.4.x<br>• 23.3.x<br>• 23.2.x | • 1.14.6<br>• 1.11.8 | • 1.27.x<br>• 1.26.x<br>• 1.25.x | 23.4.x | 23.4.x | 23.4.x |
| **SEPP** | 23.4.2 | • 23.4.x<br>• 23.3.x<br>• 23.2.x | • 23.4.x<br>• 23.3.x<br>• 23.2.x | • 23.4.x<br>• 23.3.x<br>• 23.2.x | 23.4.x | 1.14.6 | • 1.27.x<br>• 1.26.x<br>• 1.25.x | 23.4.x | NA | NA |

**Table 3-2 (Cont.) Compatibility Matrix**

| CNC NF | NF Version | CNE | cnDBTier | CDCS | OSO | ASM S/W | Kubernetes | CNC Console | OCNADD | OCCM |
|---|---|---|---|---|---|---|---|---|---|---|
| **SEPP** | 23.4.1 | • 23.4.x<br>• 23.3.x<br>• 23.2.x | • 23.4.x<br>• 23.3.x<br>• 23.2.x | • 23.4.x<br>• 23.3.x<br>• 23.2.x | 23.3.x | 1.14.6 | • 1.27.x<br>• 1.26.x<br>• 1.25.x | 23.4.x | NA | NA |
| **SEPP** | 23.4.0 | • 23.4.x<br>• 23.3.x<br>• 23.2.x | • 23.4.x<br>• 23.3.x<br>• 23.2.x | • 23.4.x<br>• 23.3.x<br>• 23.2.x | 23.3.x | 1.14.6 | • 1.27.x<br>• 1.26.x<br>• 1.25.x | 23.4.x | NA | NA |
| **UDR** | 23.4.2 | • 23.4.x<br>• 23.3.x<br>• 23.2.x | • 23.4.x<br>• 23.3.x<br>• 23.2.x | NA | • 23.4.x<br>• 23.3.x<br>• 23.2.x | • 1.14.6<br>• 1.11.8 | • 1.27.x<br>• 1.26.x<br>• 1.25.x | 23.4.x | NA | NA |
| **UDR** | 23.4.1 | • 23.4.x<br>• 23.3.x<br>• 23.2.x | • 23.4.x<br>• 23.3.x<br>• 23.2.x | NA | • 23.4.x<br>• 23.3.x<br>• 23.2.x<br>• 22.3.x | • 1.14.6<br>• 1.11.8 | • 1.27.x<br>• 1.26.x<br>• 1.25.x | 23.4.x | NA | NA |
| **UDR** | 23.4.0 | • 23.4.x<br>• 23.3.x<br>• 23.2.x | • 23.4.x<br>• 23.3.x<br>• 23.2.x | NA | • 23.4.x<br>• 23.3.x<br>• 23.2.x<br>• 22.3.x | • 1.14.6<br>• 1.11.8 | • 1.27.x<br>• 1.26.x<br>• 1.25.x | 23.4.x | NA | 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** | 23.4.x | • 3GPP TS 23.501 v17.7.0<br>• 3GPP TS 23.502 v17.7<br>• 3GPP TS 23.503 V17.7<br>• 3GPP TS 29.500 v17.7.0<br>• 3GPP TS 29.510 v17.7<br>• 3GPP TS 29.513 V17.7<br>• 3GPP TS 29.521 v17.7.0<br>• 3GPP TS 33.501 V17.7.0 |
| **CDCS** | 23.4.x | NA |
| **CNC Console** | 23.4.x | NA |
| **CNE** | 23.4.x | NA |
| **cnDBTier** | 23.4.x | NA |
| **NEF** | 23.4.x | • 3GPP TS 29.122 v16.10.0, 17.10.0<br>• 3GPP TS 23.222 v16.9.0<br>• 3GPP TS 23.501 v16.10.0<br>• 3GPP TS 23.502 v16.10.0<br>• 3GPP TS 29.514 v16.10.0<br>• 3GPP TS 29.521 v16.10<br>• 3GPP TS 29.503 v16.14.0<br>• 3GPP TS 29.515 v16.7<br>• 3GPP TS 29.222 v16.5.0<br>• 3GPP TS 29.500 v16.6.0<br>• 3GPP TS 29.501 v16.6.0<br>• 3GPP TS 29.522 v16.10.0, 17.10.0<br>• 3GPP TS 29.510 v16.6.0<br>• 3GPP TS 29.591 v16.3.0<br>• 3GPP TS 29.518 v16.14.0<br>• 3GPP TS 33.501 v17.7.0<br>• 3GPP TS 29.504 v16.10.0<br>• 3GPP TS 29.519 v16.11.0<br>• 3GPP TS 29.508 v16.11.0<br>• 3GPP TS 23.682 v16.9.0<br>• 3GPP TS 29.337 v16.1.0<br>• 3GPP TS 29.214 v16.7.0<br>• 3GPP TS 32.291 v16.14<br>• 3GPP TS 32.290 v16.10.0<br>• 3GPP TS 32.254 v16.6.0 |

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

| CNC NF | NF Version | 3GPP |
|---|---|---|
| **NEF** | 23.4.x | • 3GPP TS 29.122 v16.10.0, 17.10.0<br>• 3GPP TS 23.222 v16.9.0<br>• 3GPP TS 23.501 v16.10.0<br>• 3GPP TS 23.502 v16.10.0<br>• 3GPP TS 29.514 v16.10.0<br>• 3GPP TS 29.521 v16.10<br>• 3GPP TS 29.503 v16.14.0<br>• 3GPP TS 29.515 v16.7<br>• 3GPP TS 29.222 v16.5.0<br>• 3GPP TS 29.500 v16.6.0<br>• 3GPP TS 29.501 v16.6.0<br>• 3GPP TS 29.522 v16.10.0, 17.10.0<br>• 3GPP TS 29.510 v16.6.0<br>• 3GPP TS 29.591 v16.3.0<br>• 3GPP TS 29.518 v16.14.0<br>• 3GPP TS 33.501 v17.7.0<br>• 3GPP TS 29.504 v16.10.0<br>• 3GPP TS 29.519 v16.11.0<br>• 3GPP TS 29.508 v16.11.0<br>• 3GPP TS 23.682 v16.9.0<br>• 3GPP TS 29.337 v16.1.0<br>• 3GPP TS 29.214 v16.7.0<br>• 3GPP TS 32.291 v16.14<br>• 3GPP TS 32.290 v16.10.0<br>• 3GPP TS 32.254 v16.6.0 |
| **NRF** | 23.4.x | • 3GPP TS 29.510 v15.5<br>• 3GPP TS 29.510 v16.3.0<br>• 3GPP TS 29.510 v16.7 |
| **NSSF** | 23.4.x | • 3GPP TS 29.531 v15.5.0<br>• 3GPP TS 29.531 v16.5.0<br>• 3GPP TS 29.531 v16.8.0<br>• 3GPP TS 29.501 v16.10.0<br>• 3GPP TS 29.502 v16.10.0 |
| **OCCM** | 23.4.x | • 3GPP TS 33.310-h30<br>• 3GPP TR 33.876 v.0.3.0 |

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

| CNC NF | NF Version | 3GPP |
|---|---|---|
| **Policy** | 23.4.x | • 3GPP TS 33.501 v17.7.0<br>• 3GPP TS 29.500v16.9.0<br>• 3GPP TS 23.501v16.9.0<br>• 3GPP TS 23.502v16.9.0<br>• 3GPP TS 23.503v16.9.0<br>• 3GPP TS 29.504v16.9.0<br>• 3GPP TS 29.507v16.9.0<br>• 3GPP TS 29.510v16.9.0<br>• 3GPP TS 29.512v16.14<br>• 3GPP TS 29.513v16.9.0<br>• 3GPP TS 29.514v16.14.0<br>• 3GPP TS 29.214v16.5.0<br>• 3GPP TS 29.518v16.13.0<br>• 3GPP TS 29.519v16.8<br>• 3GPP TS 29.520v16.8<br>• 3GPP TS 29.521v16.8.0<br>• 3GPP TS 29.525v16.9.0<br>• 3GPP TS 29.594v16.7<br>• 3GPP TS 23.203 v16.2.0<br>• 3GPP TS 29.212 V16.3.0<br>• 3GPP TS 29.213v16.3<br>• 3GPP TS 29.214 v16.2.0<br>• 3GPP TS 29.219 v16.0.0<br>• 3GPP TS 29.335v16.0 |
| **SCP** | 23.4.x | • 3GPP TS 29.500 R16 v16.6.0<br>• 3GPP TS 29.501 R16 v16.5.0 |
| **SEPP** | 23.4.x | • 3GPP TS 23.501 v17.6.0<br>• 3GPP TS 23.502 v17.6.0<br>• 3GPP TS 29.500 v17.8.0<br>• 3GPP TS 29.501 v17.7.0<br>• 3GPP TS 29.510 v17.7.0<br>• 3GPP TS 33.501 v17.7.0<br>• 3GPP TS 33.117 v17.1.0<br>• 3GPP TS 33.210 v17.1.0 |
| **UDR** | 23.4.x | • 3GPP TS 29.505 v15.4.0<br>• 3GPP TS 29.504 v16.2.0<br>• 3GPP TS 29.519 v16.2.0<br>• 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 3.23.4.

**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** | 23.4.4 | 23.4.7 | 23.4.10 | 23.4.10 | 23.4.3 | 23.4.10 | 23.4.2 | 23.4.7 | 23.4.7 | 23.4.2 | NA | 23.4.5 | 23.4.10 |
| **BSF** | 23.4.2 | 23.4.5 | 23.4.6 | 23.4.5 | 23.4.2 | 23.4.6 | 23.4.1 | 23.4.5 | 23.4.5 | 23.4.1 | NA | 23.4.3 | 23.4.6 |
| **BSF** | 23.4.1 | 23.4.3 | 23.4.3 | 23.4.3 | 23.4.0 | 23.4.3 | 23.4.0 | 23.4.0 | 23.4.3 | 23.4.0 | NA | 23.4.2 | 23.4.3 |
| **BSF** | 23.4.0 | 23.4.3 | 23.4.2 | 23.4.0 | 23.4.0 | 23.4.2 | 23.4.0 | 23.4.3 | 23.4.3 | 23.4.0 | NA | 23.4.2 | 23.4.2 |
| **CNC Console** | 23.4.2 | NA | NA | NA | NA | NA | 23.4.2 | NA | 23.4.7 | 23.4.2 | NA | NA | NA |
| **CNC Console** | 23.4.1 | NA | NA | NA | NA | NA | 23.4.1 | NA | 23.4.5 | 23.4.1 | NA | NA | NA |
| **CNC Console** | 23.4.0 | NA | NA | NA | NA | NA | 23.4.0 | NA | 23.4.3 | 23.4.0 | NA | NA | NA |
| **NEF** | 23.4.4 | NA | 23.4.9 | NA | 23.4.4 | 23.4.9 | 23.4.2 | 23.4.7 | 23.4.7 | 23.4.2 | NA | 23.4.5 | 23.4.9 |
| **NEF** | 23.4.3 | NA | 23.4.5 | NA | 23.4.3 | 23.4.5 | 23.4.1 | 23.4.5 | 23.4.5 | 23.4.1 | NA | 23.4.3 | 23.4.5 |
| **NEF** | 23.4.2 | NA | 23.4.0 | NA | 23.4.0 | 23.4.0 | 23.4.0 | 23.4.1 | 23.4.1 | 23.4.0 | NA | 23.4.2 | 23.4.0 |
| **NEF** | 23.4.1 | NA | 23.4.0 | NA | 23.4.0 | 23.4.0 | 23.4.0 | 23.4.1 | 23.4.1 | 23.4.0 | NA | 23.4.2 | 23.4.0 |
| **NEF** | 23.4.0 | NA | 23.4.0 | NA | 23.4.0 | 23.4.0 | 23.4.0 | 23.4.1 | 23.4.1 | 23.4.0 | NA | 23.4.2 | 23.4.0 |
| **NRF** | 23.4.4 | 23.4.7 | 23.4.9 | 23.4.0 | 23.4.3 | NA | 23.4.2 | 23.4.7 | 23.4.7 | 23.4.2 | NA | NA | 23.4.9 |
| **NRF** | 23.4.3 | 23.4.7 | 23.4.9 | 23.4.0 | 23.4.3 | NA | 23.4.2 | 23.4.7 | 23.4.7 | 23.4.2 | NA | NA | 23.4.9 |
| **NRF** | 23.4.2 | 23.4.5 | 23.4.5 | 23.4.0 | 23.4.2 | NA | 23.4.1 | 23.4.5 | 23.4.5 | 23.4.1 | NA | NA | 23.4.5 |
| **NRF** | 23.4.1 | 23.4.4 | 23.4.1 | 23.4.0 | 23.4.1 | NA | 23.4.0 | 23.4.4 | 23.4.4 | 23.4.0 | NA | NA | 23.4.1 |
| **NRF** | 23.4.0 | 23.4.3 | 23.4.1 | 23.4.0 | 23.4.0 | NA | 23.4.0 | 23.4.3 | 23.4.3 | 23.4.0 | NA | NA | 23.4.1 |
| **NSSF** | 23.4.0 | 23.4.0 | 23.4.3 | 23.4.1 | 23.4.0 | 23.4.0 | 23.4.0 | 23.4.3 | 23.4.3 | 23.4.0 | NA | 23.4.2 | 23.4.1 |
| **OCCM** | 23.4.3 | NA | NA | NA | NA | NA | 23.4.2 | NA | NA | 23.4.2 | NA | NA | NA |
| **OCCM** | 23.4.2 | NA | NA | NA | NA | NA | 23.4.1 | NA | NA | 23.4.1 | NA | NA | NA |
| **OCCM** | 23.4.1 | NA | NA | NA | NA | NA | 23.4.1 | NA | NA | 23.4.0 | NA | NA | NA |
| **OCCM** | 23.4.0 | NA | NA | NA | NA | NA | 23.4.0 | NA | NA | 23.4.0 | NA | NA | NA |
| **Policy** | 23.4.6 | 23.4.8 | 23.4.11 | 23.4.6 | 23.4.3 | 23.4.11 | 23.4.2 | 23.4.8 | 23.4.9 | 23.4.2 | NA | 23.4.6 | 23.4.11 |
| **Policy** | 23.4.5 | 23.4.8 | 23.4.11 | 23.4.6 | 23.4.3 | 23.4.11 | 23.4.2 | 23.4.8 | 23.4.8 | 23.4.2 | NA | 23.4.6 | 23.4.11 |
| **Policy** | 23.4.4 | 23.4.6 | 23.4.8 | 23.4.6 | 23.4.2 | 23.4.8 | 23.4.1 | 23.4.6 | 23.4.6 | 23.4.1 | NA | 23.4.4 | 23.4.8 |
| **Policy** | 23.4.3 | 23.4.5 | 23.4.6 | 23.4.5 | 23.4.2 | 23.4.6 | 23.4.1 | 23.4.5 | 23.4.5 | 23.4.1 | NA | 23.4.3 | 23.4.6 |
| **Policy** | 23.4.2 | 23.4.3 | 23.4.4 | 23.4.2 | 23.4.0 | 23.4.4 | 23.4.0 | 23.4.3 | 23.4.3 | 23.4.1 | NA | 23.4.2 | 23.4.4 |
| **Policy** | 23.4.1 | 23.4.3 | 23.4.2 | 23.4.2 | 23.4.0 | 23.4.2 | 23.4.0 | 23.4.3 | 23.4.3 | 23.4.0 | NA | 23.4.2 | 23.4.3 |
| **Policy** | 23.4.0 | 23.4.3 | 23.4.2 | 23.4.0 | 23.4.0 | 23.4.2 | 23.4.0 | 23.4.3 | 23.4.3 | 23.4.0 | NA | 23.4.2 | 23.4.2 |

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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **SCP** | 23.4.3 | NA | NA | 23.4.0 | 23.4.3 | NA | 23.4.2 | NA | NA | 23.4.2 | 23.4.2 | NA | NA |
| **SCP** | 23.4.2 | NA | NA | 23.4.0 | 23.4.2 | NA | 23.4.1 | NA | NA | 23.4.1 | 23.4.1 | NA | NA |
| **SCP** | 23.4.1 | NA | NA | 23.4.0 | 23.4.1 | NA | 23.4.0 | NA | NA | 23.4.0 | 23.4.0 | NA | NA |
| **SCP** | 23.4.0 | NA | NA | 23.4.0 | 23.4.0 | NA | 23.4.0 | NA | NA | 23.4.0 | 23.4.0 | NA | NA |
| **SEPP** | 23.4.2 | 23.4.7 | 23.4.9 | 23.4.0 | 23.4.2 | 23.4.9 | 23.4.2 | 23.4.7 | 23.4.7 | 23.4.2 | 23.4.2 | 23.4.5 | 23.4.9 |
| **SEPP** | 23.4.1 | 23.4.5 | 23.4.5 | 23.4.0 | 23.4.1 | 23.4.5 | 23.4.1 | 23.4.5 | 23.4.5 | 23.4.1 | 23.4.1 | 23.4.3 | 23.4.5 |
| **SEPP** | 23.4.0 | 23.4.3 | 23.4.1 | 23.4.0 | 23.4.0 | 23.4.1 | 23.4.0 | 23.4.3 | 23.4.3 | 23.4.0 | 23.4.0 | 23.4.2 | 23.4.1 |
| **UDR** | 23.4.2 | 23.4.7 | 23.4.7 | 23.4.0 | 23.4.3 | 23.4.9 | 23.4.2 | 23.4.7 | 23.4.7 | 23.4.2 | NA | 23.4.5 | 23.4.9 |
| **UDR** | 23.4.1 | 23.4.5 | 23.4.5 | 23.4.0 | 23.4.2 | 23.4.5 | 23.4.1 | 23.4.5 | 23.4.5 | 23.4.1 | NA | 23.4.3 | 23.4.5 |
| **UDR** | 23.4.0 | 23.4.3 | 23.4.2 | 23.4.0 | 23.4.0 | 23.4.2 | 23.4.0 | 23.4.3 | 23.4.3 | 23.4.0 | NA | 23.4.2 | 23.4.2 |

# 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 23.4.4**

Table 3-5 BSF Security Certification Declaration

| Compliance Test Description | Test Completion Date | Summary |
|---|---|---|
| Static Source Code Analysis<br>Additional Info: Assesses adherence to common secure coding standards | Jul 12, 2024 | No unmitigated critical or high findings |
| Dynamic Analysis (including fuzz testing)<br>Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25 | Jul 08, 2024 | No unmitigated critical or high findings |
| Vulnerability Scans<br>Additional Info: Scans for CVEs in embedded 3rd party components | Jul 12, 2024 | No unmitigated critical or high finding |

Table 3-5 (Cont.) BSF Security Certification Declaration

| Compliance Test Description | Test Completion Date | Summary |
|---|---|---|
| Malware Scans<br>Additional Info: Scans all deliverable software packages for the presence of known malware | Jul 25, 2024 | No findings |

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

### Release 23.4.2

Table 3-6 BSF Security Certification Declaration

| Compliance Test Description | Test Completion Date | Summary |
|---|---|---|
| Static Source Code Analysis<br>Additional Info: Assesses adherence to common secure coding standards | Feb 17, 2024 | No unmitigated critical or high findings |
| Dynamic Analysis (including fuzz testing)<br>Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25 | March 20, 2024 | No unmitigated critical or high findings |
| Vulnerability Scans<br>Additional Info: Scans for CVEs in embedded 3rd party components | April 16, 2024 | No unmitigated critical or high finding |
| Malware Scans<br>Additional Info: Scans all deliverable software packages for the presence of known malware | March 20, 2024 | No findings |

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

### Release 23.4.1

**Table 3-7 BSF Security Certification Declaration**

| Compliance Test Description | Test Completion Date | Summary |
|---|---|---|
| Static Source Code Analysis<br>Additional Info: Assesses adherence to common secure coding standards | Nov 27, 2023 | No unmitigated critical or high findings |
| Dynamic Analysis (including fuzz testing)<br>Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25 | Nov 20, 2023 | No unmitigated critical or high findings |
| Vulnerability Scans<br>Additional Info: Scans for CVEs in embedded 3rd party components | Dec 5, 2023 | No unmitigated critical or high finding |
| Malware Scans<br>Additional Info: Scans all deliverable software packages for the presence of known malware | Jan 25, 2023 | No findings |

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

### Release 23.4.0

**Table 3-8 BSF Security Certification Declaration**

| Compliance Test Description | Test Completion Date | Summary |
|---|---|---|
| Static Source Code Analysis<br>Additional Info: Assesses adherence to common secure coding standards | Nov 27, 2023 | No unmitigated critical or high findings |

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

| Compliance Test Description | Test Completion Date | Summary |
|---|---|---|
| Dynamic Analysis (including fuzz testing)<br>Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25 | Nov 20, 2023 | No unmitigated critical or high findings |
| Vulnerability Scans<br>Additional Info: Scans for CVEs in embedded 3rd party components | Dec 5, 2023 | No unmitigated critical or high finding |
| Malware Scans<br>Additional Info: Scans all deliverable software packages for the presence of known malware | Dec 14, 2023 | 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 23.4.2**

**Table 3-9 CNC Console Security Certification Declaration**

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

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

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

**Release 23.4.1**

**Table 3-10 CNC Console Security Certification Declaration**

| Compliance Test Description | Test Completion Date | Summary |
|---|---|---|
| Static Source Code Analysis<br>Additional Info: Assesses adherence to common secure coding standards | Dec 11, 2023 | No unmitigated critical or high findings |
| Dynamic Analysis (including fuzz testing)<br>Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25 | Nov 29, 2023 | No unmitigated critical or high findings |
| Vulnerability Scans<br>Additional Info: Scans for CVEs in embedded 3rd party components | Apr 15, 2024 | No unmitigated critical or high finding |
| Malware Scans<br>Additional Info: Scans all deliverable software packages for the presence of known malware | Apr 16, 2024 | No findings |

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

**Release 23.4.0**

**Table 3-11 CNC Console Security Certification Declaration**

| Compliance Test Description | Test Completion Date | Summary |
|---|---|---|
| Static Source Code Analysis<br>Additional Info: Assesses adherence to common secure coding standards | Dec 11, 2023 | No unmitigated critical or high findings |
| Dynamic Analysis (including fuzz testing)<br>Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25 | Nov 29, 2023 | No unmitigated critical or high findings |
| Vulnerability Scans<br>Additional Info: Scans for CVEs in embedded 3rd party components | Dec 7, 2023 | No unmitigated critical or high finding |
| Malware Scans<br>Additional Info: Scans all deliverable software packages for the presence of known malware | Dec 11, 2023 | 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 23.4.4**

**Table 3-12 NEF Security Certification Declaration**

| Compliance Test Description | Test Completion Date | Summary |
|---|---|---|
| Static Source Code Analysis<br>Additional Info: Assesses adherence to common secure coding standards | April 20, 2024 | No unmitigated critical or high findings |

Table 3-12 (Cont.) NEF Security Certification Declaration

| Compliance Test Description | Test Completion Date | Summary |
|---|---|---|
| Dynamic Analysis (including fuzz testing)<br>Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25 | Nov 22, 2023 | No unmitigated critical or high findings |
| Vulnerability Scans<br>Additional Info: Scans for CVEs in embedded 3rd party components | July 12, 2024 | No unmitigated critical or high finding |
| Malware Scans<br>Additional Info: Scans all deliverable software packages for the presence of known malware | July 14, 2024 | No findings |

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

**Release 23.4.3**

Table 3-13 NEF Security Certification Declaration

| Compliance Test Description | Test Completion Date | Summary |
|---|---|---|
| Static Source Code Analysis<br>Additional Info: Assesses adherence to common secure coding standards | April 20, 2024 | No unmitigated critical or high findings |
| Dynamic Analysis (including fuzz testing)<br>Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25 | Nov 22, 2023 | No unmitigated critical or high findings |

**Table 3-13 (Cont.) NEF Security Certification Declaration**

| Compliance Test Description | Test Completion Date | Summary |
|---|---|---|
| Vulnerability Scans<br>Additional Info: Scans for CVEs in embedded 3rd party components | April 20, 2024 | No unmitigated critical or high finding |
| Malware Scans<br>Additional Info: Scans all deliverable software packages for the presence of known malware | April 20, 2024 | No findings |

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

**Release 23.4.2**

**Table 3-14 NEF Security Certification Declaration**

| Compliance Test Description | Test Completion Date | Summary |
|---|---|---|
| Static Source Code Analysis<br>Additional Info: Assesses adherence to common secure coding standards | Mar 26, 2024 | No unmitigated critical or high findings |
| Dynamic Analysis (including fuzz testing)<br>Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25 | Nov 22, 2023 | No unmitigated critical or high findings |
| Vulnerability Scans<br>Additional Info: Scans for CVEs in embedded 3rd party components | Mar 26, 2024 | No unmitigated critical or high finding |
| Malware Scans<br>Additional Info: Scans all deliverable software packages for the presence of known malware | Mar 27, 2024 | No findings |

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

**Release 23.4.1**

**Table 3-15 NEF Security Certification Declaration**

| Compliance Test Description | Test Completion Date | Summary |
|---|---|---|
| Static Source Code Analysis<br>Additional Info: Assesses adherence to common secure coding standards | Dec 1, 2023 | No unmitigated critical or high findings |
| Dynamic Analysis (including fuzz testing)<br>Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25 | Nov 22, 2023 | No unmitigated critical or high findings |
| Vulnerability Scans<br>Additional Info: Scans for CVEs in embedded 3rd party components | Jan 19, 2024 | No unmitigated critical or high finding |
| Malware Scans<br>Additional Info: Scans all deliverable software packages for the presence of known malware | Jan 19, 2024 | No findings |

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

**Release 23.4.0**

**Table 3-16 NEF Security Certification Declaration**

| Compliance Test Description | Test Completion Date | Summary |
|---|---|---|
| Static Source Code Analysis<br>Additional Info: Assesses adherence to common secure coding standards | Dec 11, 2023 | No unmitigated critical or high findings |

**Table 3-16 (Cont.) NEF Security Certification Declaration**

| Compliance Test Description | Test Completion Date | Summary |
|---|---|---|
| Dynamic Analysis (including fuzz testing)<br>Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25 | Nov 22, 2023 | No unmitigated critical or high findings |
| Vulnerability Scans<br>Additional Info: Scans for CVEs in embedded 3rd party components | Dec 1, 2023 | No unmitigated critical or high finding |
| Malware Scans<br>Additional Info: Scans all deliverable software packages for the presence of known malware | Dec 3, 2023 | 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 23.4.4**

**Table 3-17 NRF Security Certification Declaration**

| Compliance Test Description | Test Completion Date | Summary |
|---|---|---|
| Static Source Code Analysis<br>Additional Info: Assesses adherence to common secure coding standards | August 12, 2024 | No unmitigated critical or high findings |
| Dynamic Analysis (including fuzz testing)<br>Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25 | August 12, 2024 | No unmitigated critical or high findings |

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

| Compliance Test Description | Test Completion Date | Summary |
|---|---|---|
| Vulnerability Scans<br>Additional Info: Scans for CVEs in embedded 3rd party components | August 12, 2024 | No unmitigated critical or high finding |
| Malware Scans<br>Additional Info: Scans all deliverable software packages for the presence of known malware | August 12, 2024 | No findings |

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

### Release 23.4.3

**Table 3-18 NRF Security Certification Declaration**

| Compliance Test Description | Test Completion Date | Summary |
|---|---|---|
| Static Source Code Analysis<br>Additional Info: Assesses adherence to common secure coding standards | July 12, 2024 | No unmitigated critical or high findings |
| Dynamic Analysis (including fuzz testing)<br>Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25 | July 12, 2024 | No unmitigated critical or high findings |
| Vulnerability Scans<br>Additional Info: Scans for CVEs in embedded 3rd party components | July 12, 2024 | No unmitigated critical or high finding |
| Malware Scans<br>Additional Info: Scans all deliverable software packages for the presence of known malware | July 12, 2024 | No findings |

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

### Release 23.4.2

**Table 3-19 NRF Security Certification Declaration**

| Compliance Test Description | Test Completion Date | Summary |
|---|---|---|
| Static Source Code Analysis<br>Additional Info: Assesses adherence to common secure coding standards | Apr 18, 2024 | No unmitigated critical or high findings |
| Dynamic Analysis (including fuzz testing)<br>Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25 | Apr 18, 2024 | No unmitigated critical or high findings |
| Vulnerability Scans<br>Additional Info: Scans for CVEs in embedded 3rd party components | Apr 18, 2024 | No unmitigated critical or high finding |
| Malware Scans<br>Additional Info: Scans all deliverable software packages for the presence of known malware | Apr 18, 2024 | No findings |

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

### Release 23.4.1

**Table 3-20 NRF Security Certification Declaration**

| Compliance Test Description | Test Completion Date | Summary |
|---|---|---|
| Static Source Code Analysis<br>Additional Info: Assesses adherence to common secure coding standards | Nov 30, 2023 | No unmitigated critical or high findings |

Table 3-20 (Cont.) NRF Security Certification Declaration

| Compliance Test Description | Test Completion Date | Summary |
|---|---|---|
| Dynamic Analysis (including fuzz testing)<br>Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25 | Nov 30, 2023 | No unmitigated critical or high findings |
| Vulnerability Scans<br>Additional Info: Scans for CVEs in embedded 3rd party components | Nov 30, 2023 | No unmitigated critical or high finding |
| Malware Scans<br>Additional Info: Scans all deliverable software packages for the presence of known malware | Nov 30, 2023 | No findings |

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

**Release 23.4.0**

Table 3-21 NRF Security Certification Declaration

| Compliance Test Description | Test Completion Date | Summary |
|---|---|---|
| Static Source Code Analysis<br>Additional Info: Assesses adherence to common secure coding standards | Nov 30, 2023 | No unmitigated critical or high findings |
| Dynamic Analysis (including fuzz testing)<br>Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25 | Nov 30, 2023 | No unmitigated critical or high findings |

**Table 3-21 (Cont.) NRF Security Certification Declaration**

| Compliance Test Description | Test Completion Date | Summary |
|---|---|---|
| Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components | Nov 30, 2023 | No unmitigated critical or high finding |
| Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware | Nov 30, 2023 | No findings |

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

## 3.5.5 NSSF

**Table 3-22 NSSF Security Certification Declaration**

| Compliance Test Description | Test Completion Date | Summary |
|---|---|---|
| Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards | Dec 1, 2023 | 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 | Dec 1, 2023 | No unmitigated critical or high findings |
| Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components | Dec 1, 2023 | No unmitigated critical or high finding |
| Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware | Dec 1, 2023 | 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 23.4.3**

**Table 3-23 OCCM Security Certification Declaration**

| Compliance Test Description | Test Completion Date | Summary |
|---|---|---|
| Static Source Code Analysis<br>Additional Info: Assesses adherence to common secure coding standards | Jul 04, 2024 | No unmitigated critical or high findings |
| Dynamic Analysis (including fuzz testing)<br>Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25 | Nov 20, 2023 | No unmitigated critical or high findings |
| Vulnerability Scans<br>Additional Info: Scans for CVEs in embedded 3rd party components | Jul 04, 2024 | No unmitigated critical or high finding |
| Malware Scans<br>Additional Info: Scans all deliverable software packages for the presence of known malware | Jul 04, 2024 | No findings |

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

**Release 23.4.2**

**Table 3-24 OCCM Security Certification Declaration**

| Compliance Test Description | Test Completion Date | Summary |
|---|---|---|
| Static Source Code Analysis<br>Additional Info: Assesses adherence to common secure coding standards | Apr 05, 2024 | No unmitigated critical or high findings |

Table 3-24 (Cont.) OCCM Security Certification Declaration

| Compliance Test Description | Test Completion Date | Summary |
|---|---|---|
| Dynamic Analysis (including fuzz testing)<br>Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25 | Nov 20, 2023 | No unmitigated critical or high findings |
| Vulnerability Scans<br>Additional Info: Scans for CVEs in embedded 3rd party components | Apr 05, 2024 | No unmitigated critical or high finding |
| Malware Scans<br>Additional Info: Scans all deliverable software packages for the presence of known malware | Apr 12, 2024 | No findings |

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

**Release 23.4.1**

Table 3-25 OCCM Security Certification Declaration

| Compliance Test Description | Test Completion Date | Summary |
|---|---|---|
| Static Source Code Analysis<br>Additional Info: Assesses adherence to common secure coding standards | Mar 22, 2024 | No unmitigated critical or high findings |
| Dynamic Analysis (including fuzz testing)<br>Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25 | Nov 20, 2023 | No unmitigated critical or high findings |

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

| Compliance Test Description | Test Completion Date | Summary |
|---|---|---|
| Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components | Mar 22, 2024 | No unmitigated critical or high finding |
| Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware | Mar 25, 2024 | No findings |

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

**Release 23.4.0**

Table 3-26 OCCM Security Certification Declaration

| Compliance Test Description | Test Completion Date | Summary |
|---|---|---|
| Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards | Dec 7, 2023 | 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 | Nov 20, 2023 | No unmitigated critical or high findings |
| Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components | Dec 7, 2023 | No unmitigated critical or high finding |
| Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware | Dec 7, 2023 | No findings |

## 3.5.7 Policy Security Certification Declaration

**Table 3-27 Policy 23.4.6**

| Compliance Test Description | Test Completion Date | Summary |
|---|---|---|
| Static Source Code Analysis<br>*Additional Info: Assesses adherence to common secure coding standards* | 11 Jul 2024 | No unmitigated critical or high findings |
| Dynamic Analysis (including fuzz testing)<br>*Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25* | 17 Jun 2024 | No unmitigated critical or high findings |
| Vulnerability Scans<br>*Additional Info: Scans for CVEs in embedded 3rd party components* | 20 Aug 2024 | No unmitigated critical or high findings |
| Malware Scans<br>*Additional Info: Scans all deliverable software packages for the presence of known malware* | 16 Sep 2024 | No findings |

**Table 3-28 Policy 23.4.5**

| Compliance Test Description | Test Completion Date | Summary |
|---|---|---|
| Static Source Code Analysis<br>*Additional Info: Assesses adherence to common secure coding standards* | 01 Jul 2024 | No unmitigated critical or high findings |
| Dynamic Analysis (including fuzz testing)<br>*Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25* | 20 Jun 2024 | No unmitigated critical or high findings |
| Vulnerability Scans<br>*Additional Info: Scans for CVEs in embedded 3rd party components* | 12 Jul 2024 | No unmitigated critical or high findings |
| Malware Scans<br>*Additional Info: Scans all deliverable software packages for the presence of known malware* | 09 Aug 2024 | No findings |

### Policy 23.4.4

**Table 3-29 Policy Security Certification Declaration**

| Compliance Test Description | Test Completion Date | Summary |
|---|---|---|
| Static Source Code Analysis<br>Additional Info: Assesses adherence to common secure coding standards | Jun 11, 2024 | No unmitigated critical or high findings |
| Dynamic Analysis (including fuzz testing)<br>Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25 | May 07, 2024 | No unmitigated critical or high findings |
| Vulnerability Scans<br>Additional Info: Scans for CVEs in embedded 3rd party components | Jun 17, 2024 | No unmitigated critical or high finding |
| Malware Scans<br>Additional Info: Scans all deliverable software packages for the presence of known malware | Jun 17, 2024 | No findings |

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

### Policy 23.4.3

**Table 3-30 Policy Security Certification Declaration**

| Compliance Test Description | Test Completion Date | Summary |
|---|---|---|
| Static Source Code Analysis<br>Additional Info: Assesses adherence to common secure coding standards | Feb 17, 2024 | No unmitigated critical or high findings |

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

| Compliance Test Description | Test Completion Date | Summary |
|---|---|---|
| Dynamic Analysis (including fuzz testing)<br>Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25 | March 20, 2024 | No unmitigated critical or high findings |
| Vulnerability Scans<br>Additional Info: Scans for CVEs in embedded 3rd party components | April 16, 2024 | No unmitigated critical or high finding |
| Malware Scans<br>Additional Info: Scans all deliverable software packages for the presence of known malware | March 20, 2024 | No findings |

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

### Policy 23.4.2

**Table 3-31 Policy Security Certification Declaration**

| Compliance Test Description | Test Completion Date | Summary |
|---|---|---|
| Static Source Code Analysis<br>Additional Info: Assesses adherence to common secure coding standards | Mar 6, 2024 | No unmitigated critical or high findings |
| Dynamic Analysis (including fuzz testing)<br>Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25 | Nov 20, 2023 | No unmitigated critical or high findings |

**Table 3-31 (Cont.) Policy Security Certification Declaration**

| Compliance Test Description | Test Completion Date | Summary |
|---|---|---|
| Vulnerability Scans<br>Additional Info: Scans for CVEs in embedded 3rd party components | Mar 18, 2024 | No unmitigated critical or high finding |
| Malware Scans<br>Additional Info: Scans all deliverable software packages for the presence of known malware | Mar 27, 2024 | No findings |

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

### Policy 23.4.1

**Table 3-32 Policy Security Certification Declaration**

| Compliance Test Description | Test Completion Date | Summary |
|---|---|---|
| Static Source Code Analysis<br>Additional Info: Assesses adherence to common secure coding standards | Nov 27, 2023 | No unmitigated critical or high findings |
| Dynamic Analysis (including fuzz testing)<br>Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25 | Nov 14, 2023 | No unmitigated critical or high findings |
| Vulnerability Scans<br>Additional Info: Scans for CVEs in embedded 3rd party components | Dec 5, 2023 | No unmitigated critical or high finding |
| Malware Scans<br>Additional Info: Scans all deliverable software packages for the presence of known malware | Feb 7, 2023 | No findings |

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

### Policy 23.4.0

**Table 3-33 Policy Security Certification Declaration**

| Compliance Test Description | Test Completion Date | Summary |
|---|---|---|
| Static Source Code Analysis<br>Additional Info: Assesses adherence to common secure coding standards | Nov 29, 2023 | No unmitigated critical or high findings |
| Dynamic Analysis (including fuzz testing)<br>Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25 | Nov 14, 2023 | No unmitigated critical or high findings |
| Vulnerability Scans<br>Additional Info: Scans for CVEs in embedded 3rd party components | Dec 4, 2023 | No unmitigated critical or high finding |
| Malware Scans<br>Additional Info: Scans all deliverable software packages for the presence of known malware | Dec 14, 2023 | 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 23.4.3**

**Table 3-34    SCP Security Certification Declaration**

| Compliance Test Description | Test Completion Date | Summary |
|---|---|---|
| Static Source Code Analysis<br>Additional Info: Assesses adherence to common secure coding standards | July 16, 2024 | No unmitigated critical or high findings |
| Dynamic Analysis (including fuzz testing)<br>Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25 | July 16, 2024 | No unmitigated critical or high findings |
| Vulnerability Scans<br>Additional Info: Scans for CVEs in embedded 3rd party components | July 16 2024 | No unmitigated critical or high finding |
| Malware Scans<br>Additional Info: Scans all deliverable software packages for the presence of known malware | July 16, 2024 | No findings |

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

**SCP 23.4.2**

**Table 3-35    SCP Security Certification Declaration**

| Compliance Test Description | Test Completion Date | Summary |
|---|---|---|
| Static Source Code Analysis<br>Additional Info: Assesses adherence to common secure coding standards | April 18, 2024 | No unmitigated critical or high findings |

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

| Compliance Test Description | Test Completion Date | Summary |
|---|---|---|
| Dynamic Analysis (including fuzz testing)<br>Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25 | April 18, 2024 | No unmitigated critical or high findings |
| Vulnerability Scans<br>Additional Info: Scans for CVEs in embedded 3rd party components | April 18, 2024 | No unmitigated critical or high finding |
| Malware Scans<br>Additional Info: Scans all deliverable software packages for the presence of known malware | April 18, 2024 | No findings |

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

**SCP 23.4.1**

**Table 3-36 SCP Security Certification Declaration**

| Compliance Test Description | Test Completion Date | Summary |
|---|---|---|
| Static Source Code Analysis<br>Additional Info: Assesses adherence to common secure coding standards | Dec 1, 2023 | No unmitigated critical or high findings |
| Dynamic Analysis (including fuzz testing)<br>Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25 | Dec 1, 2023 | No unmitigated critical or high findings |

**Table 3-36 (Cont.) SCP Security Certification Declaration**

| Compliance Test Description | Test Completion Date | Summary |
|---|---|---|
| Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components | Dec 1, 2023 | No unmitigated critical or high finding |
| Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware | Dec 1, 2023 | No findings |

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

**SCP 23.4.0**

**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 | Dec 1, 2023 | 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 | Dec 1, 2023 | No unmitigated critical or high findings |
| Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components | Dec 1, 2023 | No unmitigated critical or high finding |
| Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware | Dec 1, 2023 | No findings |

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

## 3.5.9 SEPP

**Release 23.4.2**

**Table 3-38 SEPP Security Certification Declaration**

| Compliance Test Description | Test Completion Date | Summary |
|---|---|---|
| Static Source Code Analysis<br>Additional Info: Assesses adherence to common secure coding standards | July 15, 2023 | No unmitigated critical or high findings. Scan done through Fortify. |
| Dynamic Analysis (including fuzz testing)<br>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<br>Additional Info: Scans for CVEs in embedded 3rd party components | July 15, 2024 | No unmitigated critical or high findings. Scan done through Blackduck. |
| Malware Scans<br>Additional Info: Scans all deliverable software packages for the presence of known malware | July 15, 2024 | No issues found. Scan done through McAfee. |

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

**Release 23.4.1**

**Table 3-39 SEPP Security Certification Declaration**

| Compliance Test Description | Test Completion Date | Summary |
|---|---|---|
| Static Source Code Analysis<br>Additional Info: Assesses adherence to common secure coding standards | April 12, 2024 | No unmitigated critical or high findings. Scan done through Fortify. |

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

| Compliance Test Description | Test Completion Date | Summary |
|---|---|---|
| Dynamic Analysis (including fuzz testing)<br>Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25 | April 12, 2024 | No unmitigated critical, high, medium, and low findings. Scan done through RestFuzz. |
| Vulnerability Scans<br>Additional Info: Scans for CVEs in embedded 3rd party components | April 12, 2024 | No unmitigated critical or high findings. Scan done through Blackduck. |
| Malware Scans<br>Additional Info: Scans all deliverable software packages for the presence of known malware | April 12, 2024 | No issues found. Scan done through McAfee. |

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

**Release 23.4.0**

**Table 3-40 SEPP Security Certification Declaration**

| Compliance Test Description | Test Completion Date | Summary |
|---|---|---|
| Static Source Code Analysis<br>Additional Info: Assesses adherence to common secure coding standards | Dec 6, 2023 | No unmitigated critical or high findings. Scan done through Fortify. |
| Dynamic Analysis (including fuzz testing)<br>Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25 | Dec 6, 2023 | No unmitigated critical, high, medium, and low findings. Scan done through RestFuzz. |

**Table 3-40 (Cont.) SEPP Security Certification Declaration**

| Compliance Test Description | Test Completion Date | Summary |
|---|---|---|
| Vulnerability Scans<br>Additional Info: Scans for CVEs in embedded 3rd party components | Dec 6, 2023 | No unmitigated critical or high findings. Scan done through Blackduck. |
| Malware Scans<br>Additional Info: Scans all deliverable software packages for the presence of known malware | Dec 6, 2023 | 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

**UDR 23.4.2**

**Table 3-41 UDR Security Certification Declaration**

| Compliance Test Description | Test Completion Date | Summary |
|---|---|---|
| Static Source Code Analysis<br>Additional Info: Assesses adherence to common secure coding standards | June 12, 2024 | No unmitigated critical or high findings |
| Dynamic Analysis (including fuzz testing)<br>Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25 | June 12, 2024 | No unmitigated critical or high findings |
| Vulnerability Scans<br>Additional Info: Scans for CVEs in embedded 3rd party components | June 12, 2024 | No unmitigated critical or high finding |

Table 3-41 (Cont.) UDR Security Certification Declaration

| Compliance Test Description | Test Completion Date | Summary |
|---|---|---|
| Malware Scans<br>Additional Info: Scans all deliverable software packages for the presence of known malware | June 12, 2024 | No findings |

### UDR 23.4.1

Table 3-42 UDR Security Certification Declaration

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

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

### UDR 23.4.0

**Table 3-43 UDR Security Certification Declaration**

| Compliance Test Description | Test Completion Date | Summary |
|---|---|---|
| Static Source Code Analysis<br>Additional Info: Assesses adherence to common secure coding standards | Nov 24, 2023 | No unmitigated critical or high findings |
| Dynamic Analysis (including fuzz testing)<br>Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25 | Nov 24, 2023 | No unmitigated critical or high findings |
| Vulnerability Scans<br>Additional Info: Scans for CVEs in embedded 3rd party components | Nov 28, 2023 | No unmitigated critical or high finding |
| Malware Scans<br>Additional Info: Scans all deliverable software packages for the presence of known malware | Dec 4, 2023 | 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) 3.23.4 are available for download on SecureSites and MOS.

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

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

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

4

# Resolved and Known Bugs

This chapter lists the resolved and known bugs for Oracle Communications Cloud Native Core release 3.23.4.

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

## 4.1 Severity Definitions

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

**Severity 1**

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

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

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

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

**Severity 2**

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

**Severity 3**

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

**Severity 4**

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

# 4.2 Resolved Bug List

The following Resolved Bugs tables list the bugs that are resolved in Oracle Communications Cloud Native Core Release 3.23.4.

## 4.2.1 BSF Resolved Bugs

**Table 4-1 BSF 23.4.4 Resolved Bugs**

| Bug Number | Title | Description | Severity | Found In Release |
|---|---|---|---|---|
| 36762406 | [BSF] [Oauth] experiencing Binding Create & Delete requests are failing with error 403 Forbidden, when Oauth feature & ASM is enabled on BSF | On enabling ASM and BSF OAuth feature, the binding create and delete requests were failing with 403 forbidden error. | 3 | 24.1.0 |
| 36733044 | [BSF] Egress traffic failing after Policy 23.4.2 Upgrade | With Policy upgrade to 23.4.2, Egress Gateway was failing to send outgoing traffic towards SMF, UDR, CHF, BSF and other services. | 3 | 23.4.2 |
| 36817909 | [BSF]: PCF site was affected due to EGW Memory utilization, EGW http2.remote_reset | The PCF site was impacted due to high rate of unexpected abort exceptions resulting in performance and latency degradation of the Egress Gateway. | 4 | 23.4.3 |

**Note:**

Resolved bugs from 23.4.2 have been forward ported to Release 23.4.4.

**Table 4-2 BSF 23.4.2 Resolved Bugs**

| Bug Number | Title | Description | Severity | Found In Release |
|---|---|---|---|---|
| 36394528 | BSF binding response adding "null" response for sd | BSF binding response was adding a "null" response for the sd parameter. | 2 | 23.2.0 |
| 36293417 | BSF 23.4.0 is not providing ALPN TLS extension in Server Hello message | BSF was not providing ALPN TLS extension in the Server Hello message. | 2 | 23.4.0 |

Table 4-2 (Cont.) BSF 23.4.2 Resolved Bugs

| Bug Number | Title | Description | Severity | Found In Release |
|---|---|---|---|---|
| 35885521 | BSF 23.2.0 SCP Monitoring via Health API not working | The Health API for SCP Monitoring failed to function properly. | 2 | 23.2.0 |
| 36400949 | OCBSF:2.4.0 SNMP MIB file error observed | Obsolete file imports were causing issues with mib validations. | 3 | 23.4.0 |

**Note:**

Resolved bugs from 23.4.1 have been forward ported to Release 23.4.2.

Table 4-3 BSF ATS 23.4.2 Resolved Bugs

| Bug Number | Title | Description | Severity | Found In Release |
|---|---|---|---|---|
| 36323413 | BSF_ATS_23.4.0 Unexpected behavior of service account in stub deployment | ServiceAccount creation flag was not being considered in python-stub helm charts. | 3 | 23.4.0 |

Table 4-4 BSF 23.4.1 Resolved Bugs

| Bug Number | Title | Description | Severity | Found In Release |
|---|---|---|---|---|
| 36158189 | CHF connector HTTP2 Remote Reset causing N28 create failure | CHF connector was failing with concurrent modification exception during validation of SBI binding header value while sending request messages with 3GPP SBI binding header. | 2 | 22.2.3 |

**Note:**

Resolved bugs from 23.4.0 have been forward ported to Release 23.4.1.

**Table 4-5 BSF 23.4.0 Resolved Bugs**

| Bug Number | Title | Description | Severity | Found In Release |
|---|---|---|---|---|
| 35977483 | BSF - Mandatory AVP: Auth-Application-Id missing in 5012 - DIAMETER_UNABLE_TO_COMPLY | Diameter Gateway did not send Auth-Application-Id AVP in AAA response with default/configurable diameter error code, when diameter pods were in partial shutdown state. | 2 | 23.1.3 |
| 35683072 | Ingress Gateway, Binding, Deregister fails; 404 errors | PCF Binding Service did not delete binding records from its database when there was a 404 NOT_FOUND failure response from BSF for binding de-register requests. | 2 | 22.3.1 |
| 35826040 | Wrong metrics name used in Dashboard 22.3.4 BSF documentation | Though BSF KPI Dashboard file was used for Grafana, some of the BSF metrics which got pegged due to nomenclature, were not displayed. | 3 | 22.3.5 |
| 35491923 | Alert fired DBTierDownAlert Though DB service is up | `DBTeirDownAlert` and `AppInfoBsfDown` alerts were being triggered even though the database was up and running. As a result, BSF was not registered with NRF. | 3 | 23.1.1 |
| 35791394 | Prod - BSF - Ingress Error Rate alerts | Ingress Error Rate alerts were generated due to missing *namespace* or *instance*. | 3 | 23.1.2 |
| 35293896 | BSF Bulk Export Request not exporting all selected configurations | BSF Bulk Export request was not exporting all the selected configurations. | 3 | 22.4.2 |
| 35819164 | BSF 23.1.3 - NF Score Signaling connections score not updating after dropping a peer | For NF Scoring, the signaling connection score did not change. Additionally, the diam_peer_conn_down alert ware generated, but it did not have any impact on the alerts score as well. | 3 | 23.1.3 |
| 35849642 | Incorrect Critical alerts IngressDeleteErrorRateAboveMinorThreshold raised due to incorrect Alert | Incorrect critical alerts `IngressDeleteErrorRateAboveMinorThreshold` were raised due to incorrect Alert. | 3 | 22.3.5 |

**Table 4-5 (Cont.) BSF 23.4.0 Resolved Bugs**

| Bug Number | Title | Description | Severity | Found In Release |
|---|---|---|---|---|
| 35444780 | Session Viewer Issue for ipv6 query request in CNCC | Unable to run session viewer query with ipv6Prefix. | 3 | 23.1.1 |
| 35470708 | bsf-management failed after 22.1 to 22.3 upgrade | BSF Management serviced failed after upgrading from 22.1 to 22.3. | 3 | 22.3.1 |
| 35480108 | Calculation issue with Alert: IngressDeleteErrorRateAboveMinorThreshold | There were calculation issue with `IngressDeleteErrorRateAboveMinorThreshold` alert. | 3 | 23.1.1 |

> **Note:**
>
> Resolved bugs from 23.1.x and 23.2.x have been forward ported to Release 23.4.0.

## 4.2.2 CDCS Resolved Bugs

**Release 23.4.0**

**Table 4-6 CDCS 23.4.0 Resolved Bugs**

| Bug Number | Title | Description | Severity | Found In Release |
|---|---|---|---|---|
| 35820090 | Remove Worker Node pipeline is not waiting for pods to come up | The *hosts.ini* file was not updated after the worker node was removed as the pipeline failed before performing the operation. | 2 | 23.3.0 |
| 36090930 | Remove sourcing of openrc.sh file for CNE VMware upgrade | VMware upgrade from 23.1.x to 22.4.x and releases failed from 23.1.x to 23.2.x as the source `openrc.sh` file is used for upgrading VMware. Once the source *openrc.sh* is removed, the VMware upgrade was performed successfully. | 2 | • 23.2.1<br>• 23.3.0 |
| 35753103 | Job for ATS run failed in CDCS | ATS run failed on CDCS for SCP as Python libraries like `api4Jenkins` which used crumb request were unable to call ATS commands. | 3 | 23.3.0 |
| 36090975 | Fix Delete OCCNE release pipeline | The Delete CNE pipeline used to remove unused CNE releases from CDCS did not work as expected. | 3 | 23.3.0 |

**Table 4-6 (Cont.) CDCS 23.4.0 Resolved Bugs**

| Bug Number | Title | Description | Severity | Found In Release |
|---|---|---|---|---|
| 36090988 | Remove strict checking of ini file sections in Activate Local DNS pipeline | The activation of the local DNS pipeline from CDCS failed when *occne.ini* had multiple *occne:vars* sections. | 3 | 23.3.0 |
| 35751941 | The CDCS 23.2.1 deployment having issue with Cosmetic for GUI | Jenkins version 2.414.1 was not compatible with CDCS GUI. This version had changed its HTML structure and did not allow to use all CSS provided by the login-theme-plugin. | 4 | 23.2.1 |

## 4.2.3 CNC Console Resolved Bugs

**Table 4-7 CNC Console 23.4.2 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. | 2 | 24.2.0 |
| 36738843 | CNCC PDB ALLOWED DISRUPTIONS 0 - Kubernetes Upgrade fail | The `podDisruptionBudget` configuration had the incorrect value. | 3 | 24.1.0 |

**Note:**

Resolved bugs from 23.1.3, 23.2.1, 23.2.2, 23.3.1, 23.4.0, and 23.4.1 have been forward ported to Release 23.4.2.

**Table 4-8 CNC Console 23.4.1 Resolved Bugs**

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 36419158 | IPv6 not working on CNC Console | During the installation of CNC Console 23.4.0, users found that the IPv6 IPs were not assigned, and the CNC Console pods continued to point at IPv4. | 2 | 23.4.0 |

**Table 4-8 (Cont.) CNC Console 23.4.1 Resolved Bugs**

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 36445593 | CNCC does not show some NFs | Some NFs were not available in the Select Cluster drop-down on the CNC Console GUI. | 3 | 23.4.0 |
| 36197792 | Clarity regarding the occncc_custom_configtemplates_<marketing-release-number>.zip in the documentation | References to occncc_custom_configtemplates_<marketing-release-number>.zip and CSAR package needed to be updated. | 3 | 23.4.0 |
| 36277895 | Incorrect expression used for CnccCoreMemoryUsageCrossedCriticalThreshold alert | The expression used for the `CnccCoreMemoryUsageCrossedCriticalThreshold` alert was incorrect. | 3 | 23.4.0 |
| 36229762 | Restore Procedure needs updating/ clarifying | The Fault Recovery DB Backup and Restore procedure needed to be updated for better clarity. | 4 | 23.4.0 |
| 36275224 | CNCC 23.4 user guide documentation errors | There was a spelling error in the Oracle Communications Cloud Native Configuration Console User Guide. | 4 | 23.4.0 |

**Table 4-9 CNC Console 23.4.0 Resolved Bugs**

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 35808170 | DB Replication break after cncc upgrade from 23.2.0 to 23.3.0 | Database Replication broke when CNC Console was upgraded from 23.2.0 to 23.3.0. | 2 | 23.2.0 |
| 35938184 | Performing a helm upgrade to 23.2 on CNCC causes database replication errors | Performing a Helm upgrade to 23.3.0 in CNC Console caused database replication errors. | 2 | 23.2.0 |
| 35207194 | Observing JDBC exception after CNCC Deployment in cm-service | A JDBC exception was seen when CNC Console was deployed in cm-service. | 3 | 23.1.0 |
| 35974624 | CNCC Upgrade to 23.2.1 id failing (part of PCF 23.2.4 Upgrade) | CNC Console upgrade to 23.2.1 failed for the customer. | 3 | 23.2.1 |

**Table 4-9 (Cont.) CNC Console 23.4.0 Resolved Bugs**

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 35951110 | LDAP connection with FQDN not working. Works with IPv6. | LDAP connectivity to the customer's Active Directory server using the IPv6 address was working, however, the LDAP connection with FQDN was not working. | 3 | 23.2.1 |
| 36037941 | Single Database Restore for CNCC failing | Single Database Restore for CNC Console failed. | 3 | 23.2.0 |
| 35999652 | CNCC security content and pod security policy | CNC Console security content and pod security policy details were missing from the *Oracle Communications Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide*. | 3 | 23.1.0 |
| 35779867 | Password Expiration Policy is missing in CNCC 23.2 User Guide | The password expiration policy was missing in *Oracle Communications Cloud Native Configuration Console User Guide*. | 4 | 23.2.0 |

> **Note:**
>
> Resolved bugs from 23.1.3, 23.2.1, 23.2.2, and 23.3.1 have been forward ported to release 23.4.0.

## 4.2.4 cnDBTier Resolved Bugs

**Table 4-10 cnDBTier 23.4.6 Resolved Bugs**

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 36875962 | DIAM GW pods restarted caused site to go down due rolling restarts of DB-tier | When diameter gateway service pods restarted, it caused the cluster to go down due to cnDBTier rolling restarts. | 1 | 23.4.4 |
| 36909520 | Pre-upgrade hook job fails on a setup deployed with pod and container prefix | There was an upgrade failure in ASM environment as there were empty container names when cnDBTier was deployed with container prefix. | 2 | 24.2.0 |

**Table 4-10 (Cont.) cnDBTier 23.4.6 Resolved Bugs**

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 36745830 | cnDbtier user guide procedure to enable https over replication service is not working | User requested to document the procedure to generate PKCS12 certificate for HTTPS connection between replication services. | 3 | 23.2.3 |
| 36865230 | After upgrading DBTier to 23.4.4 replication channel broke between clusters. | After upgrading cnDBTier to 23.4.4 in a site, replication channel broke between the clusters. | 3 | 23.4.4 |

**Table 4-11 cnDBTier 23.4.5 Resolved Bugs**

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 36738924 | dbtrecover script failing for fatal recovery on HTTPS and TLS enabled CNDB setup | The `dbtrecover` script used old IP address to verify if the replica stopped. | 2 | 24.2.0 |
| 36779318 | ndbmysqld pod is restarted with EXIT Code 2 during traffic run | Biglog purging logic failed to read decimal value when decimals numbers were used in the disk size of ndbmysqld pods. | 3 | 24.2.0 |
| 36688177 | dbtrecover script failing on setup with pod and container prefix | Georeplication recovery using the `dbtrecover` script failed when the setups were configured with pod prefix. | 3 | 24.2.0 |
| 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 4-11 (Cont.) cnDBTier 23.4.5 Resolved Bugs**

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 36557242 | RestFuzz analysis on unexpected HTTP responses | cnDBTier returned incorrect HTTPS responses:<br>• The system displayed the 404 error code instead of 500 when server IDs did not exist.<br>• The system displayed the 503 or 404 error code instead of 500 in a single site setup.<br>• The system displayed the 404 error code when "backup_id" was not found in the backup transfer REST API response. | 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 |
| 36644321 | RestFuzz scan results flagged 500 Response codes | The following RestFuzz scan results flagged 500 response codes:<br>• REPLICATION_SVC_RESTFUZZ_SCAN<br>• MONITOR_SVC_RESTFUZZ_SCAN<br>• BACKUP_MANAGER_SVC_RESTFUZZ_SCAN<br>• BACKUP_EXECUTOR_SVC_RESTFUZZ_SCAN | 3 | 23.4.4 |
| 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 |
| 36753759 | Alert: BACKUP_PURGED_EARLY not coming on prometheus | The `BACKUP_PURGED_EARLY` alert did not appear on Prometheus as the alert condition was incorrect. | 3 | 24.2.0 |

Table 4-11 (Cont.) cnDBTier 23.4.5 Resolved Bugs

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 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 |
| 36689101 | Typo in documentation for alert BACKUP_TRANSFER_LOCAL_FAILED | cnDBTier documentation had a typo in the `BACKUP_TRANSFER_LOCAL_FAILED` alert name. | 4 | 24.2.0 |

Table 4-12 cnDBTier 23.4.4 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 after user creation on the multichannel cnDBTier setups deployed with pod prefix. | 2 | 24.1.0 |
| 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 |
| 36610826 | Password change not getting triggered | The `dbtpasswd` script didn't support NF password change when capital letters were used in the username and password sub-strings. | 2 | 24.1.0 |
| 36610763 | Password change not working for NF | `occneuser` was not used as the main user in the `dbtpasswd` script. | 2 | 24.1.0 |
| 36234344 | With BSF DB 23.2.2.0.0 upgrade, ndbmysqld all pods are restarting frequently | The MySQL cluster part of Binlog purging required updates to reduce the impact on Binlogging and other commands, and to improve efficiency, improve robustness, and observability. | 2 | 23.2.2 |
| 36042293 | ndbmtd pods restarted | MySQL cluster didn't accommodate Amazon Elastic File System (Amazon EFS) limitation and didn't ignore `ENOENT` error from `unlink()` system call. | 2 | 23.2.1 |

**Table 4-12 (Cont.) cnDBTier 23.4.4 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 in non-georeplication setups for `DbtierRetrieveBinLogSizeMetrics` and `DbtierRetrieveReplicationMetrics` in the monitor service. | 3 | 24.1.0 |
| 36515531 | CNDB- For ndbappmysqld pods PVC health status shows NA even when pvchealth for ndbapp is set as a true | PVC health status was not supported for `ndpapp` pods. When users set the `pvchealth` parameter for the unsupported pod (ndbapp), the status was displayed as "NA". | 3 | 24.1.0 |
| 36567611 | DB Tier Switch Over and Stop Replica API not working without "-k" flag | The CURL commands mentioned in cnDBTier documents had "`-k`" flag which can compromise the security of the system. | 3 | 24.1.0 |
| 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 |
| 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 |
| 36618788 | CNDBTier SNMP alerts: Remote site name not present in description of two alerts | Remote site name was not present in description of two alerts. | 3 | 24.1.0 |
| 36517463 | dbtrecover script continues execution post error "contact customer support to recover." | User requested to correct misleading error messages in the `dbtrecover` script output. | 3 | 24.1.0 |

Table 4-12 (Cont.) cnDBTier 23.4.4 Resolved Bugs

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 36486292 | BACKUP_TRANSFER_IN_PROGRESS alert retained on setup post remote transfer | `remote_transfer_status` didn't get updated in the database even though the backup transfer was successful. As a result, the `BACKUP_TRANSFER_IN_PROGRESS` alert was retained on setup ever after the remote transfer was completed. | 3 | 24.1.0 |
| 36482364 | No RemoteTransferStatus displayed while the backup is being transferred from data pod to replication svc | CNC Console GUI didn't display `RemoteTransferStatus` when the backup was transferred from the data pod to the replication service. | 3 | 24.1.0 |
| 36599370 | Enhance DBTRecover logs to point to exact cause of failure. | User requested to correct misleading error messages in the `dbtrecover` script output. | 4 | 24.1.0 |

Table 4-13 cnDBTier 23.4.3 Resolved Bugs

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 36271935 | Unable to do recovery with DBTRecover as wrong IP is being read in DBTRecover. | The `dbtrecover` script used old IPs to restart `db-replication-svc` pods resulting in recovery failure. | 2 | 23.4.0 |
| 36339825 | Export variables used from OCCNE | Users used `OCCNE_NAMESPACE` to perform cnDBTier procedures which wiped out CNE resources. To inform users to perform steps only on cnDBTier namespace, notes are added in the cnDBTier documents wherever necessary. | 3 | 23.4.0 |
| 35657461 | Multiple Restarts observed in ndbmysqld pods during upgrade to 23.2.1 | Replication SQL pod restarted before it came up and connected to the cluster when Aspen Mesh service was enabled. | 3 | 23.2.1 |

Table 4-13 (Cont.) cnDBTier 23.4.3 Resolved Bugs

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 36242316 | DBTier DR Script failing, unexpected number of server IDs | User requested to document the procedure to remove a site from a cnDBTier deployment. For the procedure to remove a site from a cnDBTier deployment, see *Oracle Communications Cloud Native Core, cnDBTier User Guide*. | 3 | 23.2.2 |
| 36285139 | Initiate-On-Demand-Backup for single site or Non GR NF shows 500 Error on GUI | Initiating an on-demand backup for single site or non georeplication Network Function (NF) on CNC Console resulted in 500 Error. | 3 | 24.1.0 |
| 36295676 | cnDBTier 23.4.0 Replication svc pod in Init state after upgrade from 23.2.1 | The init container of "`db-replication-svc`" failed to start when the primary host included a prefix containing digits. | 3 | 23.4.0 |
| 36265057 | Error logs observed on terminal when password script is executed with actual NF | Error logs were observed while running the `dbtpasswd` script. The `dbtpasswd` script is enhanced to provide better error handling and to roll back changes when an error occurs. | 3 | 23.4.0 |
| 36363119 | Post restart nbdmtd is not able to come up | The `nbdmtd` pod was unable to come up after a restart. | 3 | 23.2.2 |
| 36289873 | DBtier 23.4.0 User Guide Recommendations | User requested for details about metrics' dimensions and per-fragment metrics in *Oracle Communications Cloud Native Core, cnDBTier User Guide*. | 4 | 23.4.0 |
| 36401678 | DBTier 23.4.0 Clarification in Installation Guide about enableInitContainerForIpDiscovery | User requested more clarification in the `enableInitContainerForIpDiscovery` parameter documentation. | 4 | 23.4.0 |

**Table 4-14 cnDBTier 23.4.2 Resolved Bugs**

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 36229967 | cnDBTier alert rules file is incorrect for 23.4.0 release | cnDBTier alert rules file name was incorrect for release 23.4.0. | 2 | 23.4.0 |
| 36273283 | 3 sites GR replication testing faliure | Network policy did not work for replication service over IPv6. | 3 | 23.4.0 |
| 36225991 | Restart observed in all replication svc pods while deploying a 3 site 6 channel setup | The startup probe parameters to configure the waiting time were missing in the `custom_values.yaml` file for replication service pods. | 3 | 23.4.0 |
| 34997129 | Clarification on DBTier Automated Backup behavior | The timezone for the backup manager service and the executor service had to be changed to UTC timezone. | 3 | 22.4.0 |

**Table 4-15 cnDBTier 23.4.1 Resolved Bugs**

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 35956435 | Cluster failure on Mansfield Voice PCF | The `TimeBetweenWatchDogCheck` parameter had to be added and set to "800" for cnDBTier data node configuration. | 1 | 23.2.1 |
| 36170595 | cnDBTier 23.4.0 file transfer between sites has failed for IPV6 | IPv6 address formatting issue caused backup transfer failures in replication service. | 2 | 23.4.0 |
| 35913287 | Remote transfer fails as backup transfer from data to replication svc failed | The backup manager service was not able to resend the backup file if there was a deadlock in one of the executor services. | 2 | 23.3.0 |
| 36168800 | Duplicate channel_id being set for channels in 3 site 6 channel setup leading to replication break | Duplicate `channel_id` set to channels in a three site six channel setup led to replication failure. | 2 | 23.4.0 |
| 35516058 | Freshly installed 4 site 6 channel setup not stable - mySQLD pods restart due to binlog thread crash | Database monitor service restarted the replication SQL pods while installing cnDBTier even when the binlog threads were not crashed. | 2 | 23.2.0 |

Table 4-15 (Cont.) cnDBTier 23.4.1 Resolved Bugs

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 36085415 | Restart in SQL pods on Scaling down and up replicas of all Replication services | Database monitor service restarted the replication SQL pods while installing cnDBTier even when the binlog threads were not crashed. | 2 | 23.4.0 |
| 35789744 | Unable to run recovery on a 4 site multi channel setup using dbtrecover script | The `dbtpasswd` script failed when the number of replication SQL pods was greater than 10. | 2 | 23.3.0 |
| 36121890 | cndbtier_restore.sh statefulsets.apps "ndbmysqld" not found | The `cndbtier_restore.sh` script failed to run some commands if the statefulset names had a prefix. | 3 | 23.2.0 |
| 35805494 | DBTier performance following traffic migration | Database monitor service (db-monitor-svc) failed to run some queries. | 3 | 22.4.0 |
| 36103499 | Command to kill the replication svc container is failing in dbtrecover execution | When SSH connection was established, orphan processes were displayed in the database replication service pod. | 3 | 23.4.0 |
| 35504646 | Unable to run recovery via dbtrecover script on an HTTPS enabled setup | The `dbtrecover` script failed to work when https connection was enabled between two sites. | 3 | 23.2.0 |
| 36000990 | Temporary errors observed during DB restore | cnDBTier documentation had to be updated with a note to ignore temporary errors that are observed while restoring a database. | 3 | 23.3.1 |
| 36089914 | Query regarding "REPLICATION_SKIP_ERRORS_LOW" alert | The `REPLICATION_SKIP_ERRORS_LOW` alert did not get cleared after the default time limit of one hour. | 3 | 23.1.2 |
| 36176050 | DR is never marked as FAILED if backup transfer from data to replication svc failed | The fault recovery status did not get updated to the "FAILED" state if the backup transfer from data to replication service failed. | 3 | 23.4.0 |
| 36107599 | Unable to recover 2nd site when using dbtrecover | The `dbtrecover` script was unable to recover the second fatal error site. | 3 | 23.4.0 |

Table 4-15 (Cont.) cnDBTier 23.4.1 Resolved Bugs

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 36204471 | On asm enabled setup on executing dbtrecover config details are not displayed | The `dbtrecover` script failed to determine if HTTPS and database encryption are enabled in ASM clusters. | 3 | 23.4.0 |
| 36144254 | Remote transfer failed during DR where network policy feature was enabled | Remote transfer failed during fault recovery when the network policy feature was enabled as port 3306 in the network policy of data nodes for allowing egress traffic to mysql pods. | 3 | 23.4.0 |
| 36194931 | Response of Health API does not match with the DB | The `ndbmtd` node was unable to run mysql queries when network policy was enabled due to a missing port (3306) in the network policy charts of data node. Due to this, the response from health API was incorrect. | 3 | 23.4.0 |
| 36146937 | cnDBTIer 23.4.0 - DR Guide Refinement Request: 7.4.9.1 Procedure Point 2.d | The steps to get the Load Balancer IPs in the cnDBTier georeplication recovery procedures documented in *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide* had to be updated with the correct description. | 4 | 23.4.0 |

Table 4-16 cnDBTier 23.4.0 Resolved Bugs

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 35956435 | Cluster failure on Mansfield Voice PCF | cnDBTier cluster failed due to a change in the order in which database heartbeats are transmitted. | 1 | 23.2.1 |
| 35913453 | DR stuck in INITIATEBACKUP state if remote transfer has failed. | Database backup manager service failed to take any new backup when the backup transfer from a data pod to the replication service failed. | 2 | 23.3.0 |

**Table 4-16 (Cont.) cnDBTier 23.4.0 Resolved Bugs**

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 35913287 | Remote transfer fails as backup transfer from data to replication svc failed. | DB replication service deleted the backup files before transferring the backup to the remote site if the first transfer attempt failed. | 2 | 23.3.0 |
| 35956635 | Geo-Replication Recovery failed in a 4 site setup with 1 other site FAILED | Georeplication recovery was stuck in the BACKUPRESTORE state and then in the RECONFIGURE state, resulting in georeplication recovery failure in a four site setup. | 2 | 23.2.1 |
| 35899529 | PCF is not sending N28 or N36 | DB replication service failed to restart the `ndbappmysqld` pods after the georeplication recovery was complete. | 2 | 23.1.3 |
| 35899339 | SCP 23.2.0 cnDBTier 3site geo-redundant query | Some of the unused MySQL `db-monitor-svc` configurations had to be removed from the `custom_values.yaml` file. | 3 | 23.2.0 |
| 35973810 | cnDBTier 23.2.2 and 23.3.x has % missing as special character in the mksecrets.sh script | The `mksecrets.sh` had to be updated to support the "%" character in MySQL passwords. | 3 | 23.2.2 |
| 35456588 | DBTier 23.1.0: Need an update on documentation of the cnDBTier Alerts | The alert documentation in the user guide had to be updated to provide details about the recommended actions for each alert. | 3 | 23.1.0 |
| 35906173 | Timeout observed in Upgrade during Horizontal scaling procedure of ndbappmsyqld pods. | The Helm upgrade timed out when the upgrade was run simultaneously along with ndbappmysqld auto-scaling. | 3 | 23.3.0 |
| 35913513 | Correction needed in spelling in post upgrade jobs logs. | Post upgrade job logs had certain spelling errors which required correction. | 4 | 23.3.0 |
| 35975443 | Error logs being printed in db-executor svc | Unnecessary error messages were printed in the database backup manager service when there were no backup IDs to purge. | 4 | 23.3.1 |

Table 4-16 (Cont.) cnDBTier 23.4.0 Resolved Bugs

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 36030365 | cnDBTIer 23.3.0 - DR Guide Refinement Request, re: 4-Site Geo-Replication | Georeplication recovery procedures in *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide* required certain updates and corrections. | 4 | 23.3.0 |
| 36043512 | Correct spellings of logging in dbtrecover logs | dbtrecover logs had certain spelling errors which required correction. | 4 | 23.2.3 |

> **Note:**
>
> Resolved bugs from 23.2.3 and 23.3.2 have been forward ported to Release 23.4.0.

## 4.2.5 CNE Resolved Bugs

Table 4-17 CNE 23.4.6 Resolved Bugs

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 36753113 | lbvm pair is not taking traffic | Load Balancer Virtual Machine (LBVM) did not handle network traffic. To resolve this issue, the interface configuration (`ifcfg`) code had to be replaced with the `NetworkManager` code. | 3 | 23.4.4 |

Table 4-18 CNE 23.4.4 Resolved Bugs

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 36496165 | OCCNE upgrade issue from 23.3.3 to 23.4.1 | The code in the `setupUpgrade` (only run on first entry) function of the `upgrade.sh` script did not quote the LBVM string variables. This caused the setting of the variable to include only the first entry (lbvm) in the string causing upgrade issues. | 1 | 23.4.1 |

**Table 4-18 (Cont.) CNE 23.4.4 Resolved Bugs**

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 36123493 | OCCNE 22.4.3 Signalling LBVM Failed switchover | User requested to automate the cleanup script that is recommended to be run manually after a failover on a standby LBVM. | 2 | 23.1.1 |
| 36370983 | Pipeline execution failure on nvme | Oracle Linux 9 (ol9) uplift caused issues in 23.4.1 BareMetal deployment on X9-2 servers that had NVME drives. | 3 | 23.4.1 |
| 36308260 | KVM no longer accepts 'ol9' as an os-variant, causes bare-metal deploy failure | CNE BareMetal deployment created Virtual Machines (VM) using the Kernel-based Virtual Machine (KVM) os-variant parameter 'ol9'. This os-variant is no longer valid in the latest OL9 update of KVM. As a result, CNE 23.4.x deployment on BareMetal failed when the first VM was created after os_update (usually master-1, as it resides in most systems on host-1 with bastion-1). | 3 | 23.4.1 |
| 36196178 | Add Kubernetes Worker Node using addBmWorkerNode.py failed | Adding a Kubernetes worker node using the `addBmWorkerNode.py` failed as the `hosts.ini` file was not updated with the recent variables. | 3 | 23.2.5 |
| 36068408 | Grafana issues seen in 23.4.0 | Many panels in Grafana dashboards did not work as the metric expressions used for those channels were deprecated or updated. | 3 | 23.4.0 |
| 36465203 | Opensearch policy not working - Skylynx2 | OpenSearch "`hot_Warm_delete`" policy didn't work and didn't delete the indices. Cron capability is added to handle the purging of old indices in OpenSearch | 3 | 23.2.5<br>23.3.4<br>23.4.1 |

**Table 4-18 (Cont.) CNE 23.4.4 Resolved Bugs**

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 36085028 | Issues observed in Opensearch/Fluentd manually uplifted cluster with CNE 23.2.5/2.0 | OpenSearch "`hot_Warm_delete`" policy didn't work and didn't delete the indices. Cron capability is added to handle the purging of old indices in OpenSearch | 3 | 23.2.5<br>23.3.4<br>23.4.1 |

**Table 4-19 CNE 23.4.1 Resolved Bugs**

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 36123493 | Signalling LBVM Failed switchover | When there was a failover on a standby LBVM, a cleanup script was recommended to be run manually. The cleanup script is automated such that when there is a failover on a standby LBVM, the system doesn't run into issues that were caused due to stale interface entries. | 2 | 23.1.1 |
| 35761798 | Update opensearch base images with Security fixes | OpenSearch base images had to be updated with security fixes. | 2 | 23.3.4 |
| 35797949 | lb-controller Migrate configmaps to K8s secrets | Load Balancer controller (lb-controller) migrated configmaps to Kubernetes secrets. | 3 | 23.3.4 |

**Table 4-20 CNE 23.4.0 Resolved Bugs**

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 35674438 | Deployment of vCNE 23.2.0 on OpenStack fails, reports errors related to Istio, Jaeger | Istio installation failed during the installation of vCNE 23.2.0 on OpenStack. | 1 | 23.2.0 |
| 35527486 | rook-ceph pods are getting restarted | The CRDs were not created due to which the csi-snapshotter container of the `csi-cephfsplugin-provisioner` pod faced error while taking snapshots. | 2 | 22.4.3 |

Table 4-20 (Cont.) CNE 23.4.0 Resolved Bugs

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 35537118 | Unable to add additional Peer Address Pool in vcne cluster | There was an issue in adding additional Peer Address Pool (PAP) in vCNE cluster using the `addPeerAddrPools.py` script. | 2 | 23.1.0 |
| 35939310 | Steps to add worker node on Bare Metal using addBmWorkerNode.py not work | The `addBmWorkerNode.py` script failed to add worker node in a BareMetal deployment. | 2 | 23.3.1 |
| 35369547 | Target index not getting deleted as part of ILM | The targeted index got recreated automatically after deleting it. This caused issue to the user as they had to regularly monitor and manage the indexes on CNE manually. | 2 | 23.1.1 |
| 35729483 | CNE missing details on how to customize pod resources during install/ upgrade. Manually tuned pods are reverting after upgrade | Details about how to tune other pods' CPU or RAM resources to override the defaults deployed by CNE had to be documented. | 3 | 23.2.3 |
| 35722778 | Fluent-bit is unable to push logs to OpenSearch | Fluentbit encountered 403 Forbidden error when attempting to write logs to an index. | 3 | 23.2.0 |

**Note:**

Resolved bugs from 23.1.3, 23.2.5, and 23.3.3 have been forward ported to release 23.4.0.

### OSO Resolved Bugs

#### OSO 23.4.5 Resolved Bugs

There are no resolved bugs in this release.

#### OSO 23.4.4 Resolved Bugs

There are no resolved bugs in this release.

#### OSO 23.4.0 Resolved Bugs

There are no resolved bugs in this release.

## 4.2.6 NEF Resolved Bugs

**NEF 23.4.4 Resolved Bugs**

There are no resolved bugs in this release.

**NEF 23.4.3 Resolved Bugs**

There are no resolved bugs in this release.

**Table 4-21 NEF 23.4.2 Resolved Bugs**

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 36390774 | Mandatory parameter 'xnef-subscription-correlation-id' missing | When `maximumNumberOfReports` threshold was reached for a subscription, Model D related headers from ME service towards UDM were not added for Delete Subscription call. | 2 | 23.4.0 |
| 36390805 | Missing Binding Header | When enabling Model D at N51 interface, NEF was not including binding header in initial subscription at N52. | 2 | 23.4.0 |

**Table 4-22 NEF 23.4.1 Resolved Bugs**

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 36204379 | Create flow (create QoS application session) - Directly to PCRF based on configuration | This parameter was added to enable AF Session for QoS feature support specifically for 4G deployments. Helm based configuration parameter was needed to control enabling or disabling AF session with QoS feature support specifically for 4G deployments. | 3 | 23.4.0 |

**Table 4-23 NEF 23.4.0 Resolved Bugs**

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 35799523 | CNDB custom values file in the package is not having the complete yaml with all the required parameters | The CNDB custom values file in the package did not have the complete yaml with all the required parameters. | 2 | 23.3.0 |
| 35799433 | NEF-GR Site:0.5ktps traffic - Site1 traffic Loss rate is 1% during Site1 - NEF1 upgrade from 23.1.2 to 23.3.0 | While performing Site1 - NEF1 upgrade from 23.1.2 to 23.3.0, there was NEF-GR Site: 0.5 ktps traffic - Site1 traffic loss rate of 1%. | 2 | 23.3.0 |

**Table 4-23 (Cont.) NEF 23.4.0 Resolved Bugs**

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 35526054 | NEF-GR Site :0.5Ktps traffic - Site1 and Site2 traffic Loss rate is more than 1% during NEF Rollback from 23.2.0 to 23.1.2 | While performing Site1 - NEF1 or Site2 - NEF2 rollback from 23.2.0 and 23.1.2, there was traffic drop with loss rate of 1.29%. | 2 | 23.2.0 |
| 35964044 | NEF:23.3.1:AFsessionQOS: Default supported events needs to be updated in the userguide and QOSRefernce value should be Mandatory | As per NEF specification (29122), the QOSReference NEF is an optional parameter, but as per 29.502, it is a mandatory parameter. Since this as a mandatory parameter, the same had to be updated in the *Oracle Communications Cloud Native Core, Network Exposure Function User Guide*.<br>Along with this, the values for both the default events for AFsessionQOS were supposed to be updated. | 3 | 23.3.1 |
| 35957944 | NEF:23.3.1:AFsessionQOS: Notification:NEF is always sending success code even though events are not subscribed. | NEF was sending success codes and notifications even for those events that were not subscribed. | 3 | 23.3.1 |
| 35950719 | NEF ATS NewFeatures are failed when I ran the test OCNEF_ME_LossOfCon in Model A | While running the OCNEF_ME_LossOfCon test in Model A, the ATS New Feature test was failing. | 3 | 23.2.0 |
| 35944607 | Model-D: 3gpp-sbi-access-scope : - Services names should not be comma separated | While performing service support in Model D deployment, `3gpp-access-scope` parameter was sending comma separated service names. Service names should not be shared in this format. | 3 | 23.3.1 |
| 35943804 | NEF giving a 201 response. even when the numberofUEs parameter is absent from the UDM response | While establishing subscription using the ExternalGroupId, NEF was returning a 201 response even when the `numberofUEs` parameter was absent from the UDM response. | 3 | 23.3.0 |
| 35918127 | NEF : 23.3.1: First subscription after NEF upgrade always getting error "Timeout" instead of subscription success | While creating a subscribition, timeout of subscription occured even after success. An error stating that the subscription already exists occured while trying to create the same subscription again was displayed. | 3 | 23.3.1 |

**Table 4-23 (Cont.) NEF 23.4.0 Resolved Bugs**

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 35913661 | Capif:23.3.0:Curl command needs to updated for api-invoker offboarding and delete security method | The cURL commands documented for api-invoker offboarding and delete security methods needed to be updated in *Oracle Communications Cloud Native Core, Network Exposure Function User Guide*. | 3 | 23.3.0 |
| 35906721 | Capif :-23.3.0: pre-provisioning -api-invoker : phone parameter allowing invalid values and string datatype | In case of pre-provision api invoker, the invalid values such as zero and negative values were allowed for the Phone parameter. Also, data type of Phone parameter was incorrect in *Oracle Communications Cloud Native Core, Network Exposure Function User Guide*. | 3 | 23.3.0 |
| 35902007 | Capif:23.3.0:capif-security-management: Some of the datatypes are incorrect. | Data type for `securityInfo` and `interfaceDetails` parameters was incorrect in *Oracle Communications Cloud Native Core, Network Exposure Function User Guide*. | 3 | 23.3.0 |
| 35901953 | Capif:23.3.0:api-invoker-management: Some of the parameters datatype are incorrect in userguide. | Data type for `APIList`, `OnboardingInformation`, and `WebsockNotifConfig` parameters was incorrect in *Oracle Communications Cloud Native Core, Network Exposure Function User Guide*. | 3 | 23.3.0 |
| 35895268 | Capif :-23.3.0: Discovery-group : Delete discovery group curl command should be updated correctly | The cURL command for delete discovery group method needed to be updated in *Oracle Communications Cloud Native Core, Network Exposure Function User Guide*. | 3 | 23.3.0 |
| 35895225 | Capif :-23.3.0: Published-apis : Some of the parameters datatypes incorrect in userguide. | Data type for `custOpName`, `operations`, `custoperations`, `domainName`, `supportedFeatures`, and `ccfid` parameters was incorrect in *Oracle Communications Cloud Native Core, Network Exposure Function User Guide*. | 3 | 23.3.0 |

**Table 4-23 (Cont.) NEF 23.4.0 Resolved Bugs**

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 35895162 | Capif :-23.3.0: api-provider-management : apiProvFuncs should be array instead of string | Data type for `apiProvFuncs` parameter was incorrect in *Oracle Communications Cloud Native Core, Network Exposure Function User Guide*. | 3 | 23.3.0 |
| 35894365 | Device Trigger notification flow (DRR) is not mentioned in the user guide | The Device Trigger notification flow (DRR) was not mentioned in *Oracle Communications Cloud Native Core, Network Exposure Function User Guide*. | 3 | 23.3.0 |
| 35893661 | The Request Body Parameters' Data Type column Table of Device Trigger in User Guide is not in compliance with 3GPP standards. | The Request Body Parameter's data type column documented in *Oracle Communications Cloud Native Core, Network Exposure Function User Guide* was not in compliance with the 3GPP standards. | 3 | 23.3.0 |
| 35893478 | Supported Response Codes Table is missing in the User Guide for Device Trigger | The Supported Response Codes table was missing in *Oracle Communications Cloud Native Core, Network Exposure Function User Guide* for Device Trigger earlier. | 3 | 23.3.0 |
| 35893340 | NEF : 23.3.0 : AFsessison QOS : incorrect datatype mentioned in user guide for flowinfo and flowid. | Data type for `flowInfo` and `flowid` parameters was incorrect in *Oracle Communications Cloud Native Core, Network Exposure Function User Guide*. | 3 | 23.3.0 |
| 35869411 | For Monitoring event "PUT" operation is not supported but In published-apis "PUT" operation is observed. | Although PUT is not supported for Monitoring Events, PUT was present in the latest release while publishing api services. | 3 | 23.3.0 |
| 35854332 | Upgrade document should mention to configure "capifDetails.apiPrefix" as "apiRoot" in 23.3.0 yaml while upgrading from 23.1.x or 23.2.x as the default value in 23.1.x or 23.2.x is "apiRoot" but in 23.3.x the default value is "" | The upgrade document needed additional information on default value to be added on configuring capifDetails.apiPrefix as apiRoot in `oc-capif-23.3.0-custom-values.yaml`, while upgrading from 23.1.x or 23.2.x. | 3 | 23.3.0 |

**Table 4-23 (Cont.) NEF 23.4.0 Resolved Bugs**

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 35791941 | User Guide Does Not Address Alert Files Provided With Custom Templates | The Alerts section in *Oracle Communications Cloud Native Core, Network Exposure Function User Guide* needed to be updated with more specific information on both NEF and CAPIF alert files. | 3 | 23.2.0 |
| 35784353 | AFSessionQOS service response code for subscription, update subscription and Notification are not as per 3gpp std . | The subscription, update, and notification response codes for AFsession QoS were supposed to be updated in *Oracle Communications Cloud Native Core, Network Exposure Function User Guide*. | 3 | 23.3.0 |
| 35753399 | Collision of Reference-Number Diameter AVP in Device Trigger create subscription flow | There was a probability of collision due to the Reference-Number Diameter AVP value in Device Trigger create transaction flow. This would result in 4xx error response. High TPS for Device Trigger Create transactions will have higher the possibility of collision. | 3 | 23.3.0 |
| 35660656 | NEF:TLS-GR: TI subscription delete is not accepting "application/json" format. | While performing create or delete Traffic Influence (TI), subscription was rejected with "INVALID URI" for json format. | 3 | 23.2.0 |
| 35396825 | TI subscription and update subscription for UDM/UDR interaction - error code 503 sending with invalid body response | While perfoming send or update subscription using external group or subscription id and deleting the UDM and UDR stubs, unknown response body was received. | 3 | 23.1.0 |
| 35191092 | 5.4.3 Obtain Authorization:-Autorization access generated even though some of the services not requested. (Scope handling) | The access_token allowed authorization access even for wrong AEF IDs that were not listed in scope parameter. | 3 | 23.1.0 |
| 35942326 | It's incomplete the documentation to configurate multisites for CAPIF and NEF installation | The procedure to configure multisites for CAPIF and NEF installation was supposed to be documented in *Oracle Communications Cloud Native Core, Network Exposure Function Installation, Upgrade, and Fault Recovery Guide*. | 4 | 23.2.0 |

Table 4-23 (Cont.) NEF 23.4.0 Resolved Bugs

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 35754197 | Alerts for the "Add/Delete SubscriptionFailureRateCrossedThreshold" are not working. | `MEAddSubscriptionFailureRateCrossedThreshold` and `MEDeleteSubscriptionFailureRateCrossedThreshold` alerts were not displayed in Prometheus. | 4 | 23.2.0 |

## 4.2.7 NRF Resolved Bugs

Table 4-24 NRF 23.4.4 Resolved Bugs

| Bug Number | Title | Description | Severity | Found In Release |
|---|---|---|---|---|
| 36895948 | NRF Discovery requests failure after NRF upgrade to 23.4.2 | Discovery requests failed when NRF was upgraded from 23.3.2 to 23.4.2. This was due to an issue in the 23.4.x software, when a Discovery request sent a query to CDS (new microservice in 23.4.x) and when CDS queried the database for fetching the profiles, the database query failed due to an exception. This caused the discovery request to flush out all the profiles from its in-memory cache. | 1 | 23.4.4 |

**Table 4-25 NRF 23.4.3 Resolved Bugs**

| Bug Number | Title | Description | Severity | Found In Release |
|---|---|---|---|---|
| 36813295 | 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 |
| 36813314 | 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 |
| 36838558 | NfStatusSubscribe has high latency when subscriptionLimit feature is enabled | `NfStatusSubscribe` had high latency when subscriptionLimit feature was enabled. | 3 | 24.1.0 |
| 36838563 | 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 |

Table 4-25    (Cont.) NRF 23.4.3 Resolved Bugs

| Bug Number | Title | Description | Severity | Found In Release |
|---|---|---|---|---|
| 36838565 | 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 |
| 36753852 | NRF 23.4.1: 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 |
| 36838567 | 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 |
| 36838570 | 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 |
| 36838571 | 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 |

### Table 4-25 (Cont.) NRF 23.4.3 Resolved Bugs

| Bug Number | Title | Description | Severity | Found In Release |
|---|---|---|---|---|
| 36732897 | OcnrfTotalNFsRegisteredBelowCriticalThreshold alert is getting raised despite NFs are registered | The non leader auditor pod did not peg the metric `ocnrf_active_registrations_count` with the value as zero. This raised the `OcnrfTotalNFsRegisteredBelowCriticalThreshold` alert. | 3 | 23.2.2 |

### Table 4-26 NRF 23.4.2 Resolved Bugs

| Bug Number | Title | Description | Severity | Found In Release |
|---|---|---|---|---|
| 36528708 | AMF responding to NRF notification with 400 BAD Request due to operation in lower case | NRF sends notificationData with profileChanges which contains operation values in lower case. It must be in upper case. | 3 | 23.4.0 |

### Table 4-27 NRF 23.4.1 Resolved Bugs

| Bug Number | Title | Description | Severity | Found In Release |
|---|---|---|---|---|
| 36275336 | NRF 23.4 No ALPN h2 in server Hello from NRF. | When mTLS is enabled in NRF, TLS Application Layer Protocol Negotiation (ALPN) extension was not returned from the NRF ingress gateway to the peer during TLS handshake. | 2 | 23.4.0 |
| 36375358 | NRF only consider a single plmn-id from nrfPlmnList to determine if a discovery request is inter-PLMN. | When more than one PLMN is configured as NRF Plan in nrfPlmnList configuration, while performing Roaming check (performed to check that the NF belongs to NRF's PLMN or not), NRF considered only the first PLMN present in the zeroth Index of nrfPlmnList. It did not use the remaining PLMN IDs configured. | 2 | 23.4.0 |

Table 4-27 (Cont.) NRF 23.4.1 Resolved Bugs

| Bug Number | Title | Description | Severity | Found In Release |
|---|---|---|---|---|
| 36375383 | NRF marking AMF deregistered momentarily while there is no HB miss & no NfDegister request sent from AMF. | When the NF (AMF in this case) sent a NfProfile Update with `nfProfileChangesSupportInd` set to true, NRF incorrectly detected the changes in service status and triggered the alerts and incorrect notifications.<br>**Note:** The NF service status did not get changed in the database and remained REGISTERED throughout which could be used for discovery as well. In this case, wrong alerts and notifications were sent. | 2 | 23.1.1 |
| 36137134 | During NRF rollback from 23.4.0 to 23.3.1, restarts are observed in perf-info pods | During rollback from 23.4.0 to 23.3.1, restart can be observed in perf-info pod. However the PODs will eventually comeup post restart. | 2 | 23.3.0 |
| 36151855 | NRF 23.4.1: The sequence in which NF profiles are returned is inconsistent across one of the sites in NRF GR setup 23.4.0. | In scenarios, where the NF Profile Update is happening when the replication status was down or toggling, then the NF Profile Order at which it is saved in the Cache got changed. The updated content were accurate in the cached, but due to replication toggling the timestamp of the record changes. As each site had different cache, it was observed that some time the sequence in which NF profiles was returned in the discovery response was different between two georedundant sites. | 3 | 23.4.0 |

Table 4-27 (Cont.) NRF 23.4.1 Resolved Bugs

| Bug Number | Title | Description | Severity | Found In Release |
|---|---|---|---|---|
| 36171747 | NRF 23.4.0 is getting upgraded successfully during post upgrade validation when table is missing or schema is incorrect for NfSubscription or NfRegistration Microservices. | NRF upgrade did not fail when the database validations were not happening, like table was missing or schema was incorrect for NfSubscription or NfRegistration Microservices. | 3 | 23.3.1 |
| 36375916 | NRF is not updating NFServiceListMap in case priority is getting updated in NFService level during preferred locality features. | When extended preferred locality feature updated the priority or load of the profiles as per the configuration, NRF updated only the priority present in nfService attribute of the profile. The `nfServiceListMap` attribute was sent as received during registration. | 3 | 23.2.2 |
| 36244881 | ocnrf_replication_status_check_total does not get scraped from the artisan pod. | `ocnrf_replication_status_check_total` did not get scraped from the artisan pod due to which `OcnrfReplicationStatusMonitoringInactive` alert was raised for the pod even if the replication is up. | 3 | 22.3.2 |
| 36215679 | Metrics are not pegging the right nfFqdn value. | A list of metrics got pegged in NRF with nfFqdn dimension as "nfFqdn" (hardcoded). It pegged the value as received in the XFCC header (if the feature is enabled). | 3 | 23.4.0 |
| 36381070 | CNDB upgrade failing from 23.3.x to 23.4.0 due to invalid format of CNDB 23.4.0 custom-yaml. | There were indentation issues as whitespace character got substituted by tab unintentionally due to which upgrade or rollback failed with yaml lint error. | 3 | 23.2.2 |

Table 4-27 (Cont.) NRF 23.4.1 Resolved Bugs

| Bug Number | Title | Description | Severity | Found In Release |
|---|---|---|---|---|
| 36190678 | NRF 23.4.1: The total active registrations count is incorrect in NRF 23.4.0. | The total active registrations count was incorrect in NRF 23.4.0<br>From Grafana, it was observed that sum of all the individual NFs' Active Registrations is not equal to Total Active Registrations. This occurred when the auditor ran in multi-pod mode and audited the registrations during the switch to the leader pod simultaneously, which resulted in an incorrect count of registrations. | 3 | 23.4.0 |
| 36381135 | NRF- Incorrect NF Profiles (Suspended) in Discovery response when Registered NFProfile matches for feature - vsmf Support-ind in discovery. | Suspended Profiles were sent as Registered (when the EmptyList feature was Enabled) in the discovery response when the registered profile met the following condition:<br>When the value of `vsmf-support-ind` is set to true and does not match, then the registered profile should be sent without `vsmf-support-ind`.<br>Discovery service was giving priority to SUSPENDED profile with matching `vsmf-support-ind` over REGISTERED profile with absent `vsmf-support-ind`. | 3 | 23.4.0 |

Table 4-28 NRF ATS 23.4.1 Resolved Bugs

| Bug Number | Title | Description | Severity | Found In Release |
|---|---|---|---|---|
| 36177400 | Failure observed in NRF 23.4.0 ATS execution of CCA header regression pipeline | The JWT used in the data file was incorrect. | 2 | 23.4.0 |

Table 4-28 (Cont.) NRF ATS 23.4.1 Resolved Bugs

| Bug Number | Title | Description | Severity | Found In Release |
|---|---|---|---|---|
| 36244954 | NRF-ATS 23.4.1 - Service Account creation issue for STUB installation in NRF-ATS 23.3.1 | ATS did not have an option for Service Account configuration in the ATS values.yaml file for Stubs. As a result, it created a default service account that didn't have necessary permission. | 3 | 23.3.1 |
| 36183248 | NRF ATS 23.4.0: One Regression feature is not getting executed through ATS GUI | The feature file name in the ATS GUI and the tag inside the feature file were not matching. | 3 | 23.4.0 |

Table 4-29 NRF 23.4.0 Resolved Bugs

| Bug Number | Title | Description | Severity | Found In Release | |
|---|---|---|---|---|---|
| 35806633 | SCP monitoring via SCP Health APIs Fails on HTTPS - ERROR Exception frame_size_error/ invalid_frame_length | NRF was not able to send SCP Health queries to SCP if mTLS was enabled between NRF and SCP. | 2 | 23.2.0 | |
| 35924817 | NRF Rejecting discovery when “allowedPlmns” does not contain the PLMN in registration profile | As per 3GPP 29510: "When included, the `allowedPlmns` attribute need not include the PLMN ID(s) registered in the `plmnList` attribute of the NF Profile, that is, the PLMN ID(s) registered in the NF Profile shall be considered to be allowed to access the service instance." NRF was not considering own PLMN 234/10 as allowed. | 2 | 23.2.1 | |
| 36137134 | During NRF rollback from 23.4.0 to 23.3.1, restarts are observed in perf-info pods | During rollback from 23.4.0 to 23.3.1, restart can be observed in perf-info pod. However the PODs will eventually comeup post restart. | No customer impact. The pod will automatically come up post restart.<br>**Workaround**:<br>None | 2 | 23.3.0 |

Table 4-29 (Cont.) NRF 23.4.0 Resolved Bugs

| Bug Number | Title | Description | Severity | Found In Release |
|---|---|---|---|---|
| 30164410 | NF screening Error Code for Rejection set to 500 is allowing the screening | When the ErrorAction was set as `SendError` and `ErrorCode` was set as 500 for NFScreening feature, NRF allowed the messages even if the screening failed, instead of rejecting the message. | 3 | 1.2.0 |
| 35041949 | NRF should validate the SubscriptionData values | NRF was accepting invalid attributes in subscription data and saving it in the database instead of ignoring the invalid attributes. | 3 | 22.4.0 |
| 35485212 | NRF 22.4.0: NfListRetrieval With Invalid Query Parameter Returns 200 OK and Full UriList | NRF was sending the entire UriList for an invalid response received from the `NfListRetrieval` service operation. The invalid response had text beyond the parameter separator, question mark "?" in URI, that did not match "nf-type" or "limit" as defined in 3GPP TS29.510. | 3 | 22.4.0 |
| 35593334 | Incorrect value of "ocnrf_active_registrations_count" is observed. | During the auditor pod switchover scenario, in certain cases, it was observed that both the auditor pods of NRF were running as active pods and pegged the metrics. The values were read from both auditor pods which resulted in a double value of active registered profiles in NRF. | 3 | 23.2.0 |
| 35634381 | "ocnrf_nfRegister_requests_perSnssai_total" metric is getting pegged with invalid snssai format. | When an invalid snssai format was received in the registration request, the registration failed but the "`ocnrf_nfRegister_requests_perSnssai_total`" metric got pegged with an invalid format of sNssais. | 3 | 23.2.0 |

**Table 4-29 (Cont.) NRF 23.4.0 Resolved Bugs**

| Bug Number | Title | Description | Severity | Found In Release |
|---|---|---|---|---|
| 35666135 | aud claim validation {PCF,NRF} failed in CCA header for feature | When more than one NF was present in the aud claim and NRF was not present in the first index, the CCA header validation failed. | 3 | 23.2.0 |
| 35668046 | alert/metric not coming incase of multiple root certificate in ocingress-secret for feature | Only one `oc_ingressgateway_cca_certificate_info` metric was pegged with the expiry time of one of the root caroot.cer certificates when the CCA header was validated for mutiple consumer NFs. Expiry of individual certificate in metric `oc_ingressgateway_cca_certificate_info` should be pegged. | 3 | 23.2.0 |
| 35668117 | NRF- alert/metric not coming incase of multiple root certificate in ocingress-secret for feature By editing ocingress-secret to add/ modify root certificate not working for feature - CCA Header Validation | When the ocingress-secret is running, newly added or modified root certificate was not picked by NRF. | 3 | 23.2.0 |
| 35672554 | NRF- Missing mandatory "Subject claim" validation failed with incorrect Error cause "Internal Server Error" for feature - CCA Header Validation | NRF sends an internal error in the response when access token request was received with CCA header with missing mandatory parameter 'sub' in jwt claims instead of sending an error response as missing mandatory parameter. | 3 | 23.2.0 |
| 35697852 | Typo in NRF Rest Specification Guide leading to configuration failure | The SBIRoutingFilter attribute name was incorrect in the Oracle Communications Cloud Native Core, Network Repository Function REST Specification Guide. | 3 | 23.2.0 |

Table 4-29 (Cont.) NRF 23.4.0 Resolved Bugs

| Bug Number | Title | Description | Severity | Found In Release |
|---|---|---|---|---|
| 35720009 | NRF 23.2.0 Alerts Firing Due To Multiple nrfAuditor Pods | Deployments operating with more than one nrfAuditor pod fired alerts for conditions that do not exist as non-Leader nrfAuditor pod was returning a value of 0 for certain metrics. For example, Critical Alert `OcnrfRegisteredPCFsBelowCriticalThreshold` did not fire for the NRF's nrfauditor pod identified as Leader (as determined by table leaderElectionDB.NrfAuditorLeaderPod) when the non-zero value based on scraped metric `ocnrf_active_registrations_count` was returned from that pod. However, every non-Leader nrfauditor pod returned a value of "0" for that metric and consequently the Alert expression triggered the Alert. | 3 | 22.3.2 |
| 35832211 | Incorrect NFType value "UDMset" in nfSetIdList attribute of Registration Request payload for feature Limiting number of Producers | As per 3GPP specification, 3GPP TS 23.003, the <NFType> identifies the NF type of the NFs within the NF set and shall be encoded as a value of Table 6.1.6.3.3-1 of 3GPP TS 29.510 [130] but with >>>lower case characters<<<<<< Following is the Registration Payload attribute:"nfSetIdList": ["set1.UDMset.5gc.mnc014.mcc310"] is getting accepted by NRF even in upper case characters (UDM).<br>NRF was not performing case sensitive validation/comparison for the `nfSetIdList` attribute. | 3 | 23.3.0 |

Table 4-29 (Cont.) NRF 23.4.0 Resolved Bugs

| Bug Number | Title | Description | Severity | Found In Release |
|---|---|---|---|---|
| 35833051 | Incorrect Limiting NF Profiles selection when same nfsetid for 2 NFs one with lower case and other with uppercase are registered for feature Limiting number of Producers | As per 3GPP specification, 3GPP TS 23.003, 28.12, the <nfsetIdList> should be case insensitive. NRF considered this nfsetIdList as case sensitive, when there were two NF Set Ids sent with the same name but in different cases (that is, one in lower case setabc1.udms.5gc.mnc014.mcc310 and the other one in upper case setABC1.udmset.5gc.mnc014.mcc310). NRF did not return the NF profiles in the discovery response after applying the Limiting feature. | 3 | 23.3.0 |
| 35927293 | Incorrect default values under slfOptions for feature Extended Preferred Locality Based SLF Selection | Incorrect default values were present in slfOptions for Extended Preferred Locality Based SLF Selection feature in NRF Rest Specification guide. | 3 | 23.3.0 |
| 35947804 | Jaeger tracing attributes of common services like igw, egw not updated from openTracing to openTelemetry | NRF was migrated to OpenTelemetry, however the configurations continued pointing to OpenTracing. | 3 | 23.3.1 |
| 35950349 | non-adherence issues with certain cndb tier attributes' expected values | Certain cnDBTier attributes were having non-adherence issues with the expected values:<br>1. Existing value 1 for db-replication-svc / Replication-svc leader cpu cores<br>2. Existing value for `ndbconfigurations/ndb/MaxNoOfExecutionThreads` identical to ndbmtd cpu cores | 3 | 23.3.2 |

Table 4-29 (Cont.) NRF 23.4.0 Resolved Bugs

| Bug Number | Title | Description | Severity | Found In Release |
|---|---|---|---|---|
| 35959991 | ATS: Incorrect reference within their associated .feature files for 2 SCL Candidate List test file. | The two features tested in ATS runs failed the execution due to the incorrect reference within their associated .feature files. The following files: `sorted_slfCandidateListsorted_slfCandidateList01` contain feature name as `"sorted_slfCandidateList.feature"` & `"sorted_slfCandidateList.feature"` respectively. When ATS is executed, these test cases are not being run. | 3 | 23.3.1 |
| 35966966 | Upgrade/Rollback for Performance pod failing with CDCS | When NRF is upgraded from 23.2.x to 23.3.0, the upgrade failed due to the following behavior of the performance pods:<br>• It did not come up and after 11 retires, it went into the crashloopback state.<br>• It became active after 3-4 retries. | 3 | 23.3.0 |
| 35992192 | NRF returns in-correct response code for in correct method in subscription request. | When an incorrect method was sent in the Subscription requests, NRF sent an incorrect error code response as 404 instead of the correct error code "405 Method Not Allowed". | 3 | 23.3.1 |

Table 4-29 (Cont.) NRF 23.4.0 Resolved Bugs

| Bug Number | Title | Description | Severity | Found In Release |
|---|---|---|---|---|
| 36007881 | NRF syntax errors for SNMP trap MIB definition | From NRF 23.2.x, MIB files were not getting loaded into MIB browsers due to Syntax Errors. This prevented the users from monitoring NRF using the monitoring infrastructure. The syntax of MIB files was corrected by fixing the timestamp format and adding missing two objects for `NrfAlarmTableEntry` in ocnrf_mib file and one missing item added in `ocnrf_mib_tc` file. | 3 | 23.2.0 |
| 36034201 | Unable To Open MIBs In MIB Browser Or Downstream Utility | From NRF 23.2.x, MIB files were not getting loaded into MIB browsers due to Syntax Errors. This prevented the users from monitoring NRF using the monitoring infrastructure. When the syntax of MIB files was corrected by adding the END statement, these files were getting loaded in the MIB browser. | 3 | 23.2.0 |
| 36085616 | Logs are incorrectly getting reported as ERROR causing flooding of logs in Discovery pods. | Logs were incorrectly getting reported as ERROR in the discovery pods when the `targetnftype` was sent as UDR, UDM, or any other NF type that contained supi as a query parameter. This exhausted the ephemeral storage of the pod and caused a downtime of these pods. | 3 | 23.2.2 |
| 36107590 | Missing Alert notifications and attribute definition are missing in OCNRF mib files | The alert notifications for the OIDs 7096 and 7097 were missing in mib files but they were present in the alerts files. Also, the attribute definition for `ResponseReason` was missing in `mib_tc` file. | 3 | 23.2.0 |

## 4.2.8 NSSF Resolved Bugs

**Table 4-30 NSSF 23.4.0 Resolved Bugs**

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 35498800 | In Service Solution Upgrade: 2 Site GR Setup, Ingress failure (3.306% dropped on site1) observed during site 1 in service solution upgrade from CNDB version 23.1.1 to 23.2.0 | During an in-service solution upgrade at Site 1 from cnDBTier version 23.1.1 to 23.2.0, ingress failure was observed with 3.306% of traffic dropped at that site. Grafana reports a 96.694% success rate with 1.25K traffic at Site 1. | 2 | 23.2.0 |
| 35498940 | In Service Solution rollback: 2 Site GR Setup, Ingress failure (4.219% dropped on site2 and 5.607% dropped on site1) observed during in service solution rollback both sites from CNDB version 23.2.0 to 23.1.1 | During the in-service solution rollback from cnDBTier version 23.2.0 to 23.1.1 across both Site 1 and Site 2, an ingress failure was noted. Site 1 experienced a 5.607% drop, while Site 2 had a 4.219% drop in traffic. According to Grafana, Site 1 had a success rate of 94.393%, and Site 2 had a success rate of 95.781%. | 2 | 23.2.0 |
| 35845183 | NSSF 23.2.0 SCP Monitoring via Health API not working | When TLS was enabled and an inter-cluster communication took place between NSSF and SCP, there was an issue with communication for Method HTTP options. | 2 | 23.2.0 |

**Table 4-30 (Cont.) NSSF 23.4.0 Resolved Bugs**

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 35517972 | Counters are not available in Prometheus (Support for SCP Health API using HTTP2 OPTIONS) | "The following counters, namely 'oc_egressgateway_peer_health_ping_request, oc_egressgateway_peer_health_ping_response, and oc_egressgateway_peer_health_status_transitions are unavailable in Prometheus and do not display any status.As per the user guide for 23.2.0, the available counters include: peerConfiguration.healthApiPath peerMonitoringConfiguration.enabled peerMonitoringConfiguration.timeout peerMonitoringConfiguration.frequency peertMonitoringConfiguration.failureThreshold peerMonitoringConfiguration.successThreshold | 3 | 23.2.0 |
| 35684393 | NSSF 23.2 allowedNssaiList not in response when configuredsnssai has defaultIndication=true | In NSSF 23.2.0, the allowedNssaiList was not included in the response when configured snssai had the defaultIndication set to true. | 3 | 23.2.0 |

Table 4-30    (Cont.) NSSF 23.4.0 Resolved Bugs

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 35717777 | After deleting all configuration, ns-availability update delete, record is seen in snssai_list and tai_range_snssai_list_map tables | After deleting all configuration, ns-availability update, delete, record is seen in `snssai_list and tai_range_snssai_list_map` tables.<br>The SQL statement, utilized in the auth delete processing, responsible for searching records within the `tai_range_snssai_list_map` that overlap the provided tac range failed to return entries from the `tai_range_snssai_list_map` table containing single tacs that were incroporated within the TAC range. | 3 | 23.2.0 |
| 35699787 | Error statement for existing subscriber for tac 9999 & 999999 is different | When a subscription was created with a 'tac' value of '9999' while an identical subscription already existed, the NSSF threw an error stating, '"status": 422,"detail":"Failed to apply Patch : taiList should not contain duplicates","instance":"null","cause":"UNPROCESSABLE_ENTITY"}', instead of providing an error statement as '"status": 422,"detail":"Failed to apply Patch : Could not add patch Item as it already Exists.". | 3 | 23.2.0 |
| 35616274 | NSSF 23.2: The authorizedNssaiAvailabilityData includes sNSSAIs that are restricted in the TAC | In NSSF 23.2.0, the `authorizedNssaiAvailabilityData` included sNSSAIs that were restricted within the TAC. | 3 | 23.2.0 |
| 35590771 | NSSF 23.2.0 : Align error codes with 29.500 | Specific error codes either did not appear in TS 29 500 Table 5.2.7.2-1 or did not align with the expected values. | 3 | 23.2.0 |

Table 4-30 (Cont.) NSSF 23.4.0 Resolved Bugs

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 35820080 | Multiple virtual host not being configured "DNS SRV Based Selection of SCP in NSSF" NSSF 23.3.0 | Multiple virtual hosts were not configured for 'DNS SRV Based Selection of SCP in NSSF' in NSSF 23.3.0. | 3 | 23.3.0 |
| 35820053 | Requirement need to be captured in User guide "DNS SRV Based Selection of SCP in NSSF" NSSF 23.3.0 | A request was made to update the feature description for a better understanding of the DNS-SRV based selection of SCP feature and its correlation with monitoring SCPs using the health API feature. | 3 | 23.3.0 |
| 35814558 | NSSF Scaling down ingress-gateway is not changing calculated_status in appinfo | The NSSF scaling down of the ingress-gateway was not changing the `calculated_status` in appinfo because the ingress-gateway was not listed as a `critical_service` within common section in `service_categories`. | 3 | 23.2.0 |
| 35845139 | Not able to do Peer & Peer related configuration with NSSF 23.3.0 while able to do same with 23.2.0 with provided default custom file. "DNS SRV Based Selection of SCP in NSSF" | The user was unable to configure Peer and Peer-related settings with NSSF 23.3.0, whereas they were able to do it with version 23.2.0 using the provided default custom file for 'DNS SRV Based Selection of SCP' in NSSF. | 3 | 23.3.0 |
| 35739884 | After subscription , delete request is not working. It shows JDBC Error | The user successfully created subscriptions without any issues. However, when attempting to delete them, a status 500 error occurred with the reason cited as 'Unable to commit against JDBC Connection'. | 3 | 23.2.0 |
| 35776054 | While upgrading NSSF from 23.2.0 to 23.3.0 , there is no mention of creating a new database and granting access to it. | Documentation enhacement was done for highlighting that during the upgrade from NSSF 23.2.0 to 23.3.0, the user needs to create a new database and grant access to it. | 3 | 23.3.0 |

Table 4-30 (Cont.) NSSF 23.4.0 Resolved Bugs

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 35368483 | NSSF should reject the roaming scenarios because of roaming is not supported | As roaming is not supported in NSSF Release 23.1.0, if AMF sends a roaming request for PDU Session Ns-selection, NSSF should reject it. However, NSSF did not reject the request. | 3 | 23.1.0 |
| 35373599 | NSSF should reject ns-availability subscription request when AMF sends empty taiRangeList. | If AMF sends an `ns-availability subscription request` with the `supportedFeature =1` and includes the `taiRangeList` Information Element (IE), the NSSF needs to validate that at least one record is present due to the "cardinality 1..N" requirement. | 3 | 23.1.0 |
| 35846286 | NSSF ATS 23.2.0: Oauth token is corrupted 401 Error | The OAuth token was corrupted and displayed error 401. Steps were taken to generate the certificate using OpenSSL commands and create a Kubernetes secret, but an error occurred during OAuth test cases in the NewFeature file. | 3 | 23.2.0 |

Table 4-30    (Cont.) NSSF 23.4.0 Resolved Bugs

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 35899918 | NSSF 23.2.0 Installation Fail in EKS 1.25 due to PodSecurityPolicy | The user attempted to install NSSF 23.2.0 on EKS 1.25 but encountered an error due to Kubernetes v1.25, not supporting `PodSecurityPolicy` in the policy/v1beta1 version anymore. This information, found in the Kubernetes Deprecation Guide, states that `PodSecurityPolicy` is no longer served as of v1.25, causing issues for the NSSF installation. However, as the compatibility matrix in the CNC Release Notes indicated support for Kubernetes v1.25, the user faced problems installing NSSF's debug tools essential for various testing scenarios. They needed support on how to proceed with installing these tools despite the compatibility issue. | 3 | 23.3.2 |

Table 4-30 (Cont.) NSSF 23.4.0 Resolved Bugs

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 35878635 | 2GR Setup: Replication Off; NSSF should send a 404 NOT FOUND for ns-availability delete request for site2 if ns-availability put request sent to site1 | In a setup with two Geographical Redundancy (GR) instances, replication was turned off. An Ns-availability PUT request was made for Site 1, followed by an Ns-availability DELETE request for Site 2. The expected behavior was for NSSF to reject the DELETE request with a "404 Not Found" message when replication was disabled. However, it displayed a "204 No Content" message.When the GR setup was removed, the Ns-availability DELETE request triggered NSSF to correctly return a "404 NOT FOUND" message. This difference in behavior suggested a potential issue with how NSSF handled DELETE requests in the setup involving the GR instances with replication turned off. | 3 | 23.3.0 |
| 35395810 | When set nsconfig.httpMaxRetries to 3, NSSF (Discovery request) is sending 3 times towards NRF for success scenario. | During the execution of retry cases after modifying the YAML configuration (specifically altering `nsconfig.httpMaxRetries` to 3), NSSF sent three requests to NRF for a success scenario. However, in an ideal scenario, it should have sent only one request if NRF was responding with a success message. | 3 | 23.1.0 |
| 35966684 | In Subscription Patch request, if we are adding adding empty string in tac , it is getting accepted. | When handling a Subscription Patch request, the addition of an empty string in the "tac" field was being accepted without any issue. | 3 | 23.3.0 |

Table 4-30 (Cont.) NSSF 23.4.0 Resolved Bugs

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 35741361 | Indirect communication: Subscription failed when NSSF is not part of NF set & not part of GR | There was an issue where subscription failed if NSSF was not a part of the NF set or not a part of the GR, which was categorized as "Indirect communication." As per the user guide, the expected behavior was for the Subscription response to return a "201 Created" status, but is was not observed. | 3 | 23.3.0 |
| 35624980 | Site1 does not remove the NS-Availability data from the nssfProvSite1DB.tai_range_snssai_list_map table if NSSAI and taiRangeList have configured by the operator. | Two sites were configured in a 2-site GR setup, both enabled with ASM. Initially, identical data was established on both sites. Then, on Site 1, an update for network slice availability (taiRange List, previously set by the operator) was performed solely for AMF1. Following this, there was a deletion of NS-availability for both AMF1 and AMF2 on Site 1. Despite the operator's configuration of NSSAI and taiRangeList, an issue arose: the expected clearance of data in `nssfProvSite1DB.tai_range_snssai_list_map` did not occur. | 3 | 23.2.0 |

**Table 4-30 (Cont.) NSSF 23.4.0 Resolved Bugs**

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 35638572 | Discrepancy in statistics with NSSF 23.2 (Indirect communication) | There was a mismatch between the counter names expected and those found in Prometheus:<br>Expected Counter: `ocnssf_nssaiavailability_indirect_communication_rxPrometheus`Counter: Not found<br>Expected Counter: `ocnssf_nssaiavailability_indirect_communication_txPrometheus` Counter: Not found<br>Expected Counter: `ocnssf_nssaiavailability_notification_indirect_communication_txPrometheus` Counter: Not found<br>Expected Counter: `ocnssf_nssaiavailability_indirect_communication_subscription_failurePrometheus` Counter: Not found<br>Expected Counter: `ocnssf_nssaiavailability_indirect_communication_notification_failurePrometheus` Counter: Not found<br>Additionally, there is a mismatch in counter naming conventions as mentioned below:<br>User Guide Counter: `ocnssf_nssaiavailability_notification_indirect_communication_rxPrometheus` Counter: `ocnssf_nssaiavailability_notification_indirect_communication_rx_total` | 3 | 23.2.0 |

Table 4-30    (Cont.) NSSF 23.4.0 Resolved Bugs

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 35624271 | 2-site GR setup ASM Enabled: Site2 does not delete the NS-Availability information on the nssfProvSite2DB.nss rule and nssai auth tables, while Site1 deletes the NS-Availability. | In a 2-site GR setup with ASM enabled, Site2 did not delete the NS-Availability information on the `nssfProvSite2DB.nss` rule and nssai auth tables, whereas Site1 deleted the NS-Availability. | 3 | 23.2.0 |
| 35883435 | Alternate Route services work after disabling Gparam "alternateRouteServiceEnable" "DNS SRV Based Selection of SCP in NSSF" | Following the configuration of the following parameters, the lookup query functioned correctly for static data and information available in the DNS server:<br>• alternateRouteServiceEnable: set to false<br>• dnsSrvEnabled: set to true<br>. Given that the alternateRouteServiceEnable parameter was disabled, the ARS functionality should not have worked, but it was working. | 3 | 23.3.0 |
| 35814540 | Response received for ns-availability PUt Request contains TAIRangeList where start and end is same | The response obtained for the ns-availability PUT request contained a `TAIRangeList` where the start and end values were identical. | 3 | 23.2.0 |
| 35748867 | Restfuzz scan responding with non 4xx return code | Restfuzz scan responded with non 4xx return code. | 3 | 23.3.0 |
| 35570622 | NSSF package's CNDB custom yaml should be CNDB 23.2.0 rather than 23.1.0. | There was a mistake in the naming convention of the `cnDBTier-custom-values.yaml` file. | 3 | 23.2.0 |
| 35846922 | Egress pod is not updating with the Entry done in DNS server "DNS SRV Based Selection of SCP in NSSF" | The egress pod was not updating with the entry made in the DNS server for "DNS SRV Based Selection of SCP in NSSF". | 3 | 23.3.0 |
| 36029768 | NSSF 23.3.1 supported Kubernetes version inconsistency in CNE User Guide document | The Kubenetes version was incorrectly updated in the Installation Guide. | 3 | 23.3.1 |

Table 4-30 (Cont.) NSSF 23.4.0 Resolved Bugs

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 35709940 | NSSF 23.1.0 GrSite feature not exposing DELETE Method to remove a GR site | The user needed information on how to remove a 'grSite' added to the configuration. However, the DELETE method was not supported for this purpose. | 4 | 23.1.0 |
| 36088683 | In Network Slice Selection Service, User guide states Requested NSSAI is mandatory paramater, whereas in 3gpp it is marked as Optional | In the user guide, the requested NSSAI was marked as a mandatory paramater. However, according to 3GPP, it is an optional parameter. | 4 | 23.3.0 |
| 35926493 | NSSF should remove the HELM possible value of IGW pod protection in custom values yaml file. | Helm option for pod protection was not supported in NSSF 23.3.0. Despite the custom values YAML file suggesting that HELM could be used for pod protection in the Ingress Gateway, it was not supported in NSSF 23.3.0. A request was made to rectify the NSSF custom-values.yaml file. | 4 | 23.3.0 |
| 35948126 | "User agent header" Requirement page need to be updated. | "User agent header" requirement page was needed to be updated for missing scenarios. | 4 | 23.3.0 |
| 35036358 | Discovery and subscription Message Request and Response should be printed relevant DEBUG log information in OCNSSF | The Discovery and Subscription Message Requests and Responses were expected to include relevant DEBUG log information in NSSF. | 4 | 22.4.2 |

**Table 4-30 (Cont.) NSSF 23.4.0 Resolved Bugs**

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 35780106 | Ingress Gateway Replicas count in documentation and custom values Yamls are different. | The Ingress Gateway Replica count in the documentation and custom values YAML files was different. According to the documentation, the Ingress Gateway Replicas count should have been 5. However, in both the `ocnssf_asm_custom_values_23.3.0.yaml` and `ocnssf_custom_values_23.3.0.yaml` custom value files, it was set to 6. | 4 | 23.3.0 |

## 4.2.9 OCCM Resolved Bugs

**OCCM 23.4.3 Resolved Bugs**

There are no resolved bugs in this release.

**OCCM 23.4.2 Resolved Bugs**

There are no resolved bugs in this release.

> **Note:**
>
> Resolved bugs from release 23.4.0 and 23.4.1 have been forward ported to release 23.4.2.

**Table 4-31 OCCM 23.4.1 Resolved Bugs**

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 36363889 | OCCM 23.4.0: When requesting a NF certificate OCCM is sending IR with 2 SAN Extensions | OCCM included two SAN extensions in the IR while sending a request for an NF Certificate:<br>• SAN extension with the DNA ame of the OCCM.<br>• SAN extension with the relevant SAN of the NRF. | 3 | 23.4.0 |

Table 4-31 (Cont.) OCCM 23.4.1 Resolved Bugs

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 36368731 | OCCM 23.4.0: DistinguishedName is not in valid format / C=FR/OU=XYZ/ CN=Lorand RA LTE OFR LAB - Bad Request | The user received a *DistinguisgedName is not in valid format* error when an issuer was provisioned with distinguished names. | 3 | 23.4.0 |
| 36130333 | OCCM GUI lacks a mandatory check for the "Cert Type" field, leading to the Certificate page crashing in the OCCM GUI. | OCCM GUI lacks a mandatory check for the **Cert Type** field. This causes the certificate page on the OCCM GUI to crash. | 3 | 23.4.0 |

## 4.2.10 Policy Resolved Bugs

**Policy 23.4.6**

Table 4-32 Policy 23.4.6 Resolved Bugs

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 37036459 | In PCF R23.4.5 IGW is strict in requiring content-length header on POST/PUT/PATCH when a body is present | In PCF 23.4.5, the Ingress Gateway strictly requires `content-length` header attribute as part of its request body for POST/PUT/PATCH requests. | 2 | 23.4.5 |

**Note:**

Resolved bugs from 23.4.x have been forward ported to Release 23.4.6

**Policy 23.4.5**

**Table 4-33 Policy 23.4.5 Resolved Bugs**

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 36777439 | Same session ID is triggered by PCF for different subscriber - Sd interface | In a multi-pod setup, when two or more pods were restarted at the same time, the timestamp of bringing up the pod was the same in different pods. This is becasue the *sessionIds* generated had the same timestamp in hash format. | 1 | 23.4.0 |
| 36687582 | SM PCF egress traffic failing after 23.4.2 Upgrade | Egress Gateway failed to send outgoing traffic towards SMF, UDR, CHF, and BSF. | 1 | 23.4.2 |
| 36727402 | PCF AM-001 EGW 503 ERRORS | Egress Gateway displayed 503 errors for AM service requests. | 1 | 23.4.3 |
| 36785835 | PCF sending incorrect NCGI format in Rx RAR to CSCF | MCC/MNC portion of the NCGI value within *3gpp-user-location-info* of Rx RAR message was incorrectly formatted and it was sending incorrect MCC/MNC value. In the decode process, the value obtained was in incorrect format. | 2 | 23.4.0 |
| 36858015 | BSF deregistration count came to zero after upgrading PCF to v23.4.3 | Binding deregistration was not happening (count came to zero) from PCF after upgrading Policy to version 23.4.3. | 2 | 23.4.3 |

Table 4-33 (Cont.) Policy 23.4.5 Resolved Bugs

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 36732551 | cnPCF 23.4.0 // PCF PRE Pods are getting restarted on 80% Load | PRE pods were getting restarted on 80% load when traffic increased. It created a number of connections without reusing them. | 2 | 23.4.0 |
| 36847002 | Multiple STR is triggered by cnPCRF towards OCS during performance testing | Multiple Session Termination Requests (STR)s were triggered by cnPCRF towards OCS due to race condition in Gx interface. | 2 | 23.4.0 |
| 36842181 | cnPCF 23.4.0 // Egress GW removing IPv6 first hexadecimal Octet for N28 SpendingLimit request | Egress Gateway was removing IPv6 first hexadecimal Octet for N28 *SpendingLimit* request when an NF service profile was configured with an IPv6Address in IPEndPoint and that address was used while forming *tgppSbiTargetApiRootHeader* value. It was not getting converted to an HTTP format of the IPv6 address, that is, wrapped around with "[]". As a result, when Egress Gateway received a URI with IPv6 address but without square brackets around, it displayed *MalformedURLException*. | 2 | 23.4.0 |

Table 4-33 (Cont.) Policy 23.4.5 Resolved Bugs

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 36687591 | Observing PCF Sending wrong Policy triggers during call Hold | After requesting Netloc information on AAR-I or AAR-U, when an SM Update request was received with Netloc information, a RAR was triggered removing the one time trigger ANI_REPORT from SmPolicyAssociation application session information. But, the trigger ANI_REPORT was not removed from the AppSession evSubsc events as well. | 2 | 23.4.0 |
| 36798466 | Discovery cache feature: Unbounded metric "occnp_nrfclient_discovery_cache_support_cache_non_cache_total" | When Discovery cache feature was enabled and the SUPI parameter was part of the query parameters in the discovery cache, the *discovery_cache_support_cache_non_cache_total* was being exploded. | 2 | 23.4.2 |
| 36785107 | SM PCF was affected due to Memory utilization | SM-PCF was affected due to memory utilization. The memory limits on SM-PCF resulted in timeout response. | 2 | 23.2.7 |

Table 4-33 (Cont.) Policy 23.4.5 Resolved Bugs

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 36817592 | Post upgrade to 23.4.3, Policy Create, Policy Update and Policy Delete have error 403 Forbidden | After upgrading to Policy 23.4.3, the Ingress Gateway responded with 403 errors while processing SM CREATE, SM UPDATE, and SM DELETE requests. Also, UDR Connector encountered 403 errors when sending a PUT request for a subscription. | 2 | 23.4.3 |
| 36888689 | Warning message "ProducerId Header is Not present in BSF Response" | "*ProducerId Header is Not present*" warning message was missing in BSF response. | 3 | 23.4.4 |
| 36846790 | PCF is sending via header to SCP causing SCP to return 508 Loop Detected | PCF was sent through the header to SCP, causing SCP to return "*508 Loop Detected*" error. | 3 | 23.4.3 |
| 36803661 | Overload Control Discard Policy | Wrong validation range was used for route level rate and SBI discard priority. | 3 | 23.4.3 |
| 36256216 | Subscriber Activity Logs are not getting generated on Diameter Gateway and Diameter Connector Pod for Sy Interface | Subscriber activity logging header was not sent to PDS fron PCRF core. | 3 | 23.4.0 |
| 36782063 | SM-PCF sending nUDR subs-to-notify with two monitoredResourceURIs in the message - resulting in N36 setup failure | SM-PCF was sending "subs-to-notify" message to nUDR with two *monitoredResourceURIs* in the message. This resulted in N36 setup failure. | 3 | 23.4.3 |

**Table 4-33 (Cont.) Policy 23.4.5 Resolved Bugs**

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 36554674 | PCF_ATS_23.4.3 - UE_stale_session_audit feature failure | When audit deregister happened, and the response to the request was "404 NOT_FOUND", the response was processed as failure and retry the request. | 3 | 23.4.3 |
| 36577007 | Incorrect Encoding of the MNC Value in URSP Policy | When MNC contained a two digit value, there were incorrect encoding of a third digit in URSP values to '0' instead of 'F'. | 3 | 23.4.1 |
| 36751941 | Policy CV yaml needs to be updated for overload configuration | Policy *custom-values.yaml* file did not contain accurate configuration for overload to work. | 3 | 23.4.0 |
| 36765764 | nrf-client-cache shall change the Port "notused"to "http2-notused" | NRF-client was treating the incoming traffic as TCP proxy instead of HTTP2 traffic. | 3 | 23.2.7 |
| 36727124 | PCF NRF-client not updating the NF being suspended after autonomous Discovery results | NRF-client was not updating the NF being suspended after autonomous Discovery results. For example, CHF-connector was incorrectly picking up the CHF3 which was actually SUSPENDED. Also, after the request was sent to CHF3, CHF responded with 503 error. It was expected that PCF should retry to connect to the next available CHF (CHF4). However, PCF continued to connect to the first CHF (CHF3) itself. | 3 | 23.4.2 |

Table 4-33 (Cont.) Policy 23.4.5 Resolved Bugs

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 36797796 | PCF sending error 415(UNSUPPORTED_MEDIA_TYPE) for policyauthorization delete request is missing header content-type | When a POST request was received without payload, Ingress Gateway was adding content-type header with value "application/octet-stream" before forwarding that request to backend. As a result, backend service (sm-service, in this case) rejected that request with error 415 (UNSUPPORTED_MEDIA_TYPE).<br>The issue has been resolved and Ingress Gateway now does not send content-type with "application/octet-stream" as default value to backend services when the POST, PUT, and PATCH request is received without body and no content-type header in it.<br>**Note:** The POST, PUT, and PATCH HTTP requests with a body shall contain content-length header with non-zero value. | 3 | 23.1.2 |

**Note:**

Resolved bugs from 23.4.x have been forward ported to Release 23.4.5

### Policy 23.4.4

Table 4-34    Policy 23.4.4 Resolved Bugs

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 36616652 | SM PCF egress traffic failing after 23.4.2 Upgrade | With Policy upgrade from 23.2.7 to 23.4.2, Egress Gateway was failing to send outgoing traffic towards SMF, UDR, CHF, BSF and other services. | 1 | 23.4.2 |
| 36705436 | PCF AM-001 EGW 503 ERRORS | When Egress Gateway was communicating either by using SCP or without SCP, it was generating 503 service unavailable error. And PCF peer nodes were also generating 503 service unavailable error. | 2 | 23.4.3 |
| 36684612 | PCF 23.4.0 PCF is not Clearing Cache/Deleting the Suspended NF from | PCF was not clearing cache or deleting the suspended NFs such as BSF or UDR from the discovered NF list. The suspended BSF details were not present in the discovery search result received from NRF. | 2 | 23.4.0 |
| 36722873 | Performance: NFDiscovery calls are (XNIO) blocking calls to NRF in NRFDiscovery service | In NRF 23.2.2, it was observed that NFDiscovery calls from XNIO thread pool were blocking calls to NRF. | 2 | 23.2.7 |
| 36745652 | AM service is not saving the CHF response in Async CHF call flow. | The PDS was not saving the CHF *spendingLimitRequest* (SLR) object in *AmPolicyAssociation*, since the *spendingLimitInfoStatus* object was being overriden during CHF notification flow when Bulwark service was enabled. | 3 | 23.2.7 |

Table 4-34    (Cont.) Policy 23.4.4 Resolved Bugs

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 36745716 | UDR-Connector:NPE is reported when getSelfBindingHeaders() when UDR UNSUBSCRIBE is not working | The UDR put request was resulting in Null Pointer Exception (NPE) when the NF Communication Profile was configured to send binding headers. But then, the self binding headers were not present in the query. | 3 | 23.2.7 |
| 36776510 | Binding Service blocking calls are found during performance runs | Blocking calls were found in the Binding Service during performance runs. | 4 | 23.2.7 |
| 36751996 | Policy CV yaml needs to be updated for overload configuration | Policy custom_value yaml file did not have accurate information about overload control configurations. | 4 | 23.4.0 |
| 36776525 | Make boundedElastic and Underertow serever related configurations configurable through custom yaml | The *boundedElastic* and *Underertow* serever related configurations were not configurable through custom_value yaml file. | 4 | 23.2.7 |
| 36798472 | Discovery cache feature: Unbounded metric "occnp_nrfclient_discovery_cache_support_cache_non_cache_total" | When the discovery cache feature was enabled and supi parameter was part of the query parameters, there was an explosion of unbounded metric "occnp_nrfclient_discovery_cache_support_cache_non_cache_total". | 4 | 23.4.2 |
| 36765772 | nrf-client-cache shall change the Port "notused"to "http2-notused" | The nrf-client-cache should change the port from "notused" to "http2-notused". | 4 | 23.2.7 |

**Table 4-34 (Cont.) Policy 23.4.4 Resolved Bugs**

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 36681374 | Post upgrade to 23.4.3, Policy Create, Policy Update and Policy Delete have error 403 Forbidden | When the TPS was high and mutiple threads were accessing the function at same time then the JWT token was getting corrupted resulting in a malformed JWT exception on parsing. | 4 | 23.4.3 |
| 36761733 | igw-cache, egw-cache and altsvc-cache shall change the Port "notused"to "http2-notused" | During PCF and API gateway integration testing, it was observed that each Egress Gateway pods was receiving 394 incoming connections. This was happening because the Egress Gateway incoming traffic was not treated as HTTP2 connections but rather as TCP proxy connections. | 4 | 23.2.7 |
| 36741562 | SM PCF site was affected due to Memory utilization | The PCF site was impacted due to high rate of unexpected abort exceptions resulting in performance and latency degradation of the Egress Gateway. | 4 | 23.4.4 |

**Note:**

Resolved bugs from 23.4.3 have been forward ported to Release 23.4.4.

**Table 4-35 Policy 23.4.3 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 during the call hold. | 2 | 23.4.0 |

Table 4-35 (Cont.) Policy 23.4.3 Resolved Bugs

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 36331825 | PDS is not triggering SLR-Intermediate towards OCS after max session count configured is completed | The revalidation functionality (MaxSessionCount ) on custom workflow was not working properly. It was not triggering SLR-Intermediate towards OCS after max session count configured got completed. | 2 | 23.4.0 |
| 36322233 | SLR-Intermediate is not getting triggered from PDS towards OCS for second Gx session on site two PCRF | The revalidation functionality (ResetContext) on custom workflow was not working properly. SLR-Intermediate was not getting triggered from PDS towards OCS for second Gx session on site two PCRF. | 2 | 23.4.0 |
| 36399649 | Rx AARs failing with 5065 since signalling storm at 11/03 00:10 | On Converged deployment when the Rx AAR and binding service failed to determine the ContextOwner, an error response was triggered. | 2 | 23.2.4 |
| 36412828 | Observing Null pointer exception for request with invalid command code | Diameter Gateway encountered a NullPointer exception while attempting to send an error response for an unknown command, specifically when adding AuthAppId in the response. | 3 | 24.1.0 |
| 36307939 | Sy's SNRs not working when "Type of Search" is set to "Preferential Search" and GPSI in PDS Settings | Sy's SNRs failed to operate properly when the "Type of Search" was configured as "Preferential Search" and GPSI in PDS Settings. | 3 | 23.2.2 |

**Table 4-35 (Cont.) Policy 23.4.3 Resolved Bugs**

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 36442691 | 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 was not sending the RAR towards PGW at some instances. | 3 | 23.4.0 |
| 36385116 | PolicyDS generating 404 not found error for inactive Sy 4G Data cleanup | PolicyDS was generating "404 Not Found" error for inactive Sy 4G Data cleanup. | 3 | 22.4.5 |
| 36385102 | PCF-UE - Duplicate 3gpp-sbi-binding header issue | Duplicate 3gpp-sbi-binding headers were mistakenly sent towards AMF in N1N2 subscribe retry requests. | 3 | 23.2.6 |
| 36290250 | 23.4.0 cnPCRF does not send Access-Network-Charging-Address AVP in Rx AAA if address is IPv6 | cnPCRF failed to include the Access-Network-Charging-Address AVP in Rx AAA when the address was configured as IPv6. | 4 | 23.4.0 |
| 36437446 | PCF voice call issue with PolicyDS | When policyDS was disabled, no user object with userId was created. As a result, smfManager was throwing null pointer exceptions when attempting to retrieve smPolicyData from the current user. | 4 | 23.4.1 |
| 36299308 | RX and Binding sessions do not match | When PCRF-Core received cleanup request by sessionId, the session was directly deleted without proper binding cleanup. | 4 | 23.2.4 |
| 36406388 | Late Arrival Detection and Creating Record on DB after receiving SM_CREATE | PCF-SM was not deleting the older session when collision detection was enabled. | 4 | 23.4.0 |

Table 4-35 (Cont.) Policy 23.4.3 Resolved Bugs

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 36404500 | API requests to PCF GUI not responding/taking too long to respond in certain scenarios | The API requests to PCF GUI was either not responding or taking too long to respond in certain scenarios. | 4 | 23.4.0 |
| 36479043 | Invalid Value of Serving Gateway IP Address/Subnet is coming with bulk export | When an invalid Value of Serving Gateway IP Address/Subnet in pcrf-core was coming with bulk export, the IPs were not exporting or importing in a required format. | 4 | 23.4.0 |

**Note:**

Resolved bugs from 23.4.2 have been forward ported to Release 23.4.3.

Table 4-36 Policy ATS 23.4.3 Resolved Bugs

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 36415897 | PCF-ATS 23.4.1 - Newfeature failure | The NRF_Error_Mapping_Autonomous_Registration feature was failing. | 3 | 23.4.1 |
| 36211243 | PCF_ATS Unexpected behaviour of service account in stub deployment | The serviceAccount creation flag was not being considered in python-stub helm charts. | 3 | 23.4.0 |
| 36307232 | PCF ATS 23.4.1: Final run of Full Regression showing incorrect feature failures count | Regression was showing incorrect feature failures count. | 3 | 23.4.1 |
| 36290363 | Missing parametrization of Diameter_Gateway-Identity in Regression test case Emergency_Session_SSV_Off | The Diameter identity parameterization was missing in the regression test case. | 3 | 23.4.1 |

Table 4-37    Policy 23.4.2 Resolved Bugs

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 36412916 | NSA Voice calls are NOT working in the ME lab after SMF switches over | In the discovered NF profiles, PCF was identifying the 3GPP defined Standard NF service names. But it was ignoring the customized NF service names during NF profile filtering and selection from the discovered profiles from an alternate route selection. Hence, PCF was not selecting the custom NF service details and was instead using the NF level details. | 3 | 23.2.6 |
| 36390786 | Late Arrival Detection and Creating Record on DB after receiving SM_CREATE | On enabling collision detection, PCF-SM was accepting new sessions and was not deleting the older session. | 3 | 23.4.0 |
| 36401614 | Observing Null pointer exception for request with invalid command code | Diameter requests were received with invalid/unknown command code when requesting to add `AuthAppId` response parameter. At the Diameter Gateway, the requests were failing with NullPointer Exception while sending the error response. | 4 | 23.4.0 |
| 36412844 | API requests to PCF GUI not responding/taking too long to respond in certain scenarios | During function call on a established DB connection, all the threads were moving to waiting state since the synchronized keyword was used in NaN issue of the config.level metrics. | 4 | 23.4.0 |

**Note:**

Resolved bugs from 23.4.x have been forward ported to Release 23.4.2.

**Table 4-38 Policy 23.4.1 Resolved Bugs**

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 36141037 | CHF connector HTTP2 Remote Reset causing N28 create failure | CHF connector failed while processing concurrent requests of the subscribers with the concurrent modification exception. This failure happened during validation of SBI binding header value while sending CHF policy counter look up request. | 2 | 23.2.6 |
| 36100406 | PCF sending an extra UpdateNotify with partial rule content in IMS session | PCF was sending an extra UpdateNotify request with partial rule content in the IMS session. | 2 | 23.2.6 |
| 35924624 | PCF does not re-evaluate policy during pending-tx | PCF did not reevaluate the policy when the UDR or CHF notification was received during retry of an outgoing pending transaction. | 3 | 23.2.4 |
| 36220119 | Binding Registration Error due to 'too long' dependent Context Id \|\| Topology Hiding Enabled | The context_id, contextbinding_id, and dependentcontext_id column length is set to 128 in the binding service tables. As a result, when a context_id or dependent_context_id is received with a length greater than 128, the SQL error was encountered, stating "column length is exceeded. | 4 | 23.4.0 |

**Note:**

Resolved bugs from 23.4.0 have been forward ported to Release 23.4.1.

**Table 4-39 Policy 23.4.0 Resolved Bugs**

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 36060941 | Rx AAR/AAA not recorded in pcrfCore subscriber activity logging for sos call | Rx AAR/AAA was not recorded in PCRF Core subscriber activity logging. | 2 | 23.2.4 |
| 36006409 | Issue after enabling Binding SM Service TerminateNotify feature | SM Remote subscriber cleanup timed out when no associations were found. | 2 | 23.2.4 |
| 35685225 | AppInfo pods prompting error for decoding service_monitor_status.json occasionally | AppInfo pods were displaying error for decoding `service_monitor_status.json`. | 2 | 22.3.1 |
| 36034639 | Rx AAR/AAA not recorded in diamGw subscriber activity logging for sos call | Rx AAR/AAA was not recorded in Diameter Gateway subscriber activity logging. | 2 | 23.2.4 |
| 36076441 | STAGING: cnPCF 23.2.4 Sy-STR is not sent intermittently when Sd is enabled | PCRF-Core was sending unnecessary delete request to PDS and Binding service for sessions related to Sd during Sd CCR-T flow. | 2 | 23.2.4 |
| 36034681 | Sd RAR is not triggering when there is Modifying session | Gx and Sd sessions were created with IPv6 with incorrect userId values that were stored in the Sd session. | 2 | 23.2.4 |
| 36034490 | Rx Voice call is not working | Rx Voice call was not working as RAR was not sent for AAR update for changing the codecs. | 2 | 23.2.4 |
| 35513161 | Smservice and Other Pods looking for Policy-ds which is not Configured | SM service and other pods were looking for PolicyDS that was not configured. | 2 | 23.1.2 |

Table 4-39 (Cont.) Policy 23.4.0 Resolved Bugs

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 35724138 | No RAR/RAA message sent after STR message received from IMS for AF_Signalling | When the synchronous mode was enabled for the Rx session, no RAR or RAA message was sent after the STR message was received from IMS for AF_Signalling. | 2 | 23.2.0 |
| 35325827 | PCF PRE logs is not completely getting recorded in the Kibana | The PRE logs fetched using the kubectl logs command in DEBUG mode were not completely recorded in the Kibana. | 2 | 22.4.2 |
| 35351155 | SM PCF 500 errors are on Create/Delete 408 errors are on Update happening in BB | The following errors were occuring in PCF SM Service:<br>• 500 error on create or delete request<br>• 408 error on update request | 2 | 22.4.5 |
| 35421906 | No amf subscriptions on ue policy association setup | There were no AMF subscriptions on UE policy association setup. | 2 | 23.1.4 |
| 35454029 | RAR Triggered Even If there is no change in PCC Rules | RAR was triggered even If there was no change in the PCC rules. | 2 | 23.1.2 |
| 35447445 | Too many records in exception tables for pdssubscriber, pdsprofile and SmPolicyAssociation in E1 PCF | There were too many records in exception tables for pdssubscriber, pdsprofile, and SmPolicyAssociation in E1 PCF. | 2 | 22.1.1 |
| 35575690 | UDR connector prompting Error "Caught Exception while DELETE" | UDR connector was prompting the "Caught Exception while DELETE" Error. | 2 | 22.3.1 |
| 35641388 | SM-PCF Sending Traffic to an Unregistered BSF | SM-PCF was sending traffic to an unregistered BSF. | 2 | 23.1.5 |

Table 4-39 (Cont.) Policy 23.4.0 Resolved Bugs

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 35822825 | diam-gateway pod advertises cleartext HTTP port (8000) | The diam-gateway pod advertised cleartext HTTP port (8000). | 2 | 23.1.0 |
| 35857730 | subs-to-notify message with duplicate monitoredResourceUris for am-data | When AM service sent sub-to-notify request to UDR it included multiple monitored resource URIs for same resource. | 2 | 23.2.2 |
| 36028907 | Barring/unbarring of data for BTOP roaming subscribers is not working | When pcrf-core pod came up and started receiving HTTP traffic from PDS, which in turn triggered RAR even before connecting to diameter-gateway, there was a DIAMETER_UNABLE_TO_COMPLY error. | 3 | 23.2.4 |
| 35941466 | CLSP SM-PCF-AM-PCF sending duplicate monitored Resource Uris in its retry of Policy | CLSP SM-PCF-AM-PCF was sending duplicate monitored resource URIs during retry. AppInfo pods displayed errors while decoding service_monitor_status.json. | 3 | 23.1.6 |
| 35966304 | STR(Sy) message is not sent to OCS, when Sd CCR-T failed | While processing Sd requests, PCRF-Core was sending request to PDS to create Sd session. | 3 | 23.2.4 |
| 35645739 | Policy 23.2 alert query | Separate alerts for Rx STA and Sy STA messages were created. Previously, there was no protocol specific STA alert, rather it was combined as Rx and Sy which was not convenient for the metrics on the dashboard. | 3 | 23.2.0 |

Table 4-39 (Cont.) Policy 23.4.0 Resolved Bugs

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 35866991 | Observing “DiameterSessionCleanupTask” warning messages | The “DiameterSessionCleanupTask” warning message got executed by default. | 3 | 22.4.5 |
| 36023589 | TerminateNotify Feature:Binding is doing cleanup even when session gets cleanup after collisiondetection | In the TerminateNotify Feature, binding was doing cleanup even when session got cleaned up after the collision detection. | 3 | 23.2.4 |
| 36018809 | UE N1N2 Transfer Session Retry Not Working based on available AMFs. | UE N1N2 Transfer session retry was not working based on available AMFs. | 3 | 23.1.7 |
| 35955544 | Pending transaction retry with new rule contents | There were issues with AF pending transaction when there were PCC rule changes in between retries. | 4 | 23.1.7 |
| 35846823 | AAR being responded to with 5012 on Voice PCF | Pcrf-core was sending retry RAR requests continuously in a loop for more than the configured number of retries when RAA responded with DIAMETER_PENDING_TRANSACTION error code. | 4 | 22.4.6 |

**Note:**

Resolved bugs from 23.1.x and 23.2.xhave been forward ported to Release 23.4.0.

## 4.2.11 SCP Resolved Bugs

Table 4-40 SCP 23.4.3 Resolved Bugs

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 36808093 | SCP Alternate Routing using DNS SRV not working | SCP alternate routing using DNS SRV did not work when multiple API versions were present in the NF profile. | 3 | 23.4.1 |

Table 4-40 (Cont.) SCP 23.4.3 Resolved Bugs

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 36808125 | Alternate Routing using Static Configuration not working as expected | Alternate routing using static configuration did not work for the interplmn FQDN format when the corresponding NF profile was known to SCP. | 3 | 23.4.1 |
| 36808141 | Mediation rule is not triggered when user-agent header | When SCP added additional User-Agent header, it led to mediation rule failure. | 3 | 23.4.1 |
| 36808161 | SCP Feature Ignore Unknown Nf Service not working for 5G_EIR profile | SCP was unable to process the NF profile with unknown services when capacity was not defined in the profile. | 3 | 23.4.1 |
| 36810994 | SCP not able to route subsequent request for interSCP when target is FQDN | SCP was unable to route subsequent message requests for interSCP when the target was FQDN. | 3 | 23.4.2 |
| 36810864 | Avalanche of Egress request in interSCP flow even when low Ingress request | SCP retried the message request multiple times on the transport failure that resulted in a high rate of egress requests. | 3 | 23.4.2 |

**Note:**

Resolved bugs from 23.4.1 have been forward ported to release 23.4.3.

Table 4-41 SCP ATS 23.4.3 Resolved Bugs

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 36553497 | SCP_Ro_Enhancments_For_CB_CC_SMF_P0.feature is not executing all scenarios in ATS run. | SCP_Ro_Enhancments_For_CB_CC_SMF_P0.feature did not run all the scenarios in ATS. | 3 | 23.4.1 |

Table 4-42 SCP 23.4.2 Resolved Bugs

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 36532252 | SNI not sent in TLS Handshake towards Producer NF | SNI was not sent in TLS Handshake towards Producer NF. | 2 | 23.4.1 |
| 36532198 | Remove ruleApi and systemoptions helm parameters from scp deployment file | The `ruleApi` and `systemoptions` Helm parameters were removed from the SCP deployment file. | 2 | 23.4.1 |

Table 4-42 (Cont.) SCP 23.4.2 Resolved Bugs

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 36533290 | SCP: TimeoutException:Timed out waiting for a node assignment resulting in back to back scp worker restarts | The SCP-Worker pod restart was observed due to network failure or any other reachability issue from kafka broker. A lower timeout value, that is, 5 seconds for deliveryTimeoutMs avoided heap memory increase (OOM kill) in this scenario. | 2 | 24.1.0 |
| 36532205 | service-instanceID is not getting generated for nnrf-oauth2 for dynamic NRF Profiles when NRF bootstrap info enabled | service-instanceID was not getting generated for nnrf-oauth2 for dynamic NRF Profiles when NRF Bootstrap information was enabled. | 3 | 23.4.0 |
| 36532217 | Routing Config Set on Console does not have an option to enable or disable the OCI feature for notification messages. | Routing Config Set on the CNC Console did not have an option to enable or disable the OCI feature for notification messages. | 3 | 23.4.0 |
| 36532245 | SCP doesn't accept health check queries without API-Prefix and SCP send null as api-prefix when peer SCP profile does not have scp-prefix | SCP did not accept health check queries without API-Prefix, and SCP sent null as API-Prefix when the peer SCP profile did not have API-Prefix. | 3 | 23.4.1 |
| 36391134 | SCP doesn't add 3gpp-sbi-producer-id headers in response to Consumer for Inter SCP case | SCP did not add 3gpp-sbi-producer-id headers in response to consumer NFs for Inter-SCP scenarios. | 3 | 23.2.3 |
| 36390274 | SCP mediation pod part-of annotation conflicts with network-policy | The SCP mediation pod part of the annotation conflicted with network policy. | 3 | 23.2.3 |

**Note:**

Resolved bugs from 23.2.3 have been forward ported to release 23.4.2.

Table 4-43 SCP ATS 23.4.2 Resolved Bugs

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 36532176 | ATS Regression Failure - SCP_Audit_nnrf_nfm_SMF_user_agent | ATS failed when pystub terminated the connection intermittently. | 2 | 23.4.1 |
| 36532260 | OCC - Internal: SCP 23.4.1 - ModelC_CatchAll_Routing_Configuration_AUSF.feature failed | Timeout values were updated in the ATS feature files to resolve the issue. | 3 | 23.4.1 |

**Table 4-44    SCP 23.4.1 Resolved Bugs**

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 36128794 | Message Copy feature not working post upgrade from 23.3.0 to 23.4.0 | SCP was unable to connect to Kafka due to missing dependency of jgss in the SCP-Worker image. | 2 | 23.4.0 |
| 36007866 | OCI not enforced by SCP in case of received Callback URI in the response from consumer as feature enable and disable does not reset the older enforcement | When the Overload Control Information (OCI) feature was disabled, the cache did not get clear for Callback URI scope. | 2 | 23.4.0 |
| 35798556 | SCP is throttling the messages despite egress rate limit not being exceeded | SCP throttled the messages even after the egress rate limit was not exceeded. | 2 | 23.2.2 |
| 36105418 | SCP appends incorrect server header values to the oci error response while sending the response to the producer for notification messages | SCP appended incorrect server header values to the OCI error response while sending the response to the Producer NF for notification messages. | 2 | 23.4.0 |
| 36220998 | Egress host preference NF type resolution not working for HTTPS | The Egress host preference NF type resolution did not work for HTTPS. | 2 | 23.4.0 |
| 36290830 | SCP is sending 504 status code as string | SCP sent 504 status code as string in problem details. | 2 | 23.4.0 |
| 36177211 | Observed cache pod restart during the performance run with OAuth Cache enabled & Model D cache enabled | It was observed that the Cache pod restarted during a performance run with the deployment details on SCP 23.4.0. | 2 | 23.4.0 |
| 36163339 | SCP does not use routing timeout in routing options in case of InterPLMN | SCP did not use routing timeout in routing options in case of InterPLMN. | 3 | 23.4.0 |
| 36195328 | Alternate-Resolution service pod is showing high Memory Utilization | The SCP-Alternate-Resolution service pod displayed high memory utilization. | 3 | 23.4.0 |
| 36290042 | ocscp_configuration_dnssrv_nrf_duplicate_target_detected metrics and corresponding alert is not getting cleared when we delete NRF SRV FQDN in SCP | The ocscp_configuration_dnssrv_nrf_duplicate_target_detected metric and the corresponding alert were not cleared after removing NRF SRV FQDN from SCP. | 3 | 23.4.0 |
| 36257416 | SCP's DNS Srv records are retained even if the DNS SRV NRF record is deleted in the DNS Server | DNS SRV records were retained even if the DNS SRV NRF record was removed from the DNS server. | 3 | 23.4.0 |

**Note:**

Resolved bugs from 23.2.2 have been forward ported to release 23.4.1.

**Table 4-45 SCP ATS 23.4.1 Resolved Bugs**

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 36291248 | Multiple scenarios of SCP_NRFconfigurationDNSSRV_P0 feature are failing | Mutiple scenarios of the SCP_NRFconfigurationDNSSRV_P0 feature failed. | 3 | 23.4.0 |

**Table 4-46 SCP 23.4.0 Resolved Bugs**

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 36008494 | SCP does not pay attention to https schema in 3gpp-sbi-target-apiroot and try to setup http connection instead in a sub-sequent request (PDU session Update) | SCP was not taking the scheme from the `3gpp-sbi-target-apiroot` header in the request when forwarding the request to the producer. | 2 | 23.2.3 |
| 35920043 | SCP Will Not Deploy in OCI with New Operator Instance | Service signalling port was missing in the deployment file, resulting in a deployment failure in OCI. | 2 | 23.3.0 |
| 35840957 | SCP AR metric is not aligning with the RX failure responses received from producer | SCP alternate route metric was not aligned with the RX failure responses received from the producer. | 2 | 23.2.2 |
| 35835792 | SCP generated 503 & 504 errors during performance runs when Oauth2 feature is enabled and transaction rate dropped to 72% | SCP was generating a few 5xx errors during the performance run due to pod CPU overload. | 2 | 23.3.0 |
| 35798827 | Observed 429's in per pod capacity runs of Oauth feature | SCP was generating a high number of 429 errors due to pod CPU overload during the performance run. | 2 | 23.3.0 |
| 35341610 | Traffic failure(429 overload discard) was observed while running traffic at 462K/512K MPS using 8vCPU as well as 12vCPU worker pod profiles | SCP was generating a high number of 429 errors due to pod CPU overload during the performance run. | 2 | 23.1.0 |
| 35836629 | Observed that 6.7 K 429's are generated due to PendingTransactionsPercentage overload in the run where there was no delay in response at producer with Oauth2 feature enabled | SCP was generating a high number of 429 errors due to pod CPU overload during the performance run. | 2 | 23.3.0 |
| 35279002 | SCP Metrics increments host_type as "ip" in ocscp_worker_http_req_host_type_total metrics when an explicit notification with discovery headers is sent to the SCP with the Egress Host Preference feature enabled | SCP was pegging the `ocscp_worker_http_req_host_type_total` metric with an incorrect value for host_type in the case of explicit notification. | 3 | 23.1.0 |

**Table 4-46 (Cont.) SCP 23.4.0 Resolved Bugs**

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 35955854 | SCP worker pod not coming up after upgrade | Commenting out the optional parameter `sslCertExpireTimeInMin` resulted in an upgrade failure. | 3 | 23.3.1 |
| 35583607 | SCP retries same AMF two times before retrying another AMF and includes same AMF instance id multiple times in SH | SCP retried forwarding the request to the same producer twice in case the first attempt was done with the forward route. | 3 | 23.2.0 |
| 36018971 | Static Routing configuration does not work when routeGroupType is FQDN | Static Routing configuration did not work when routeGroupType was FQDN. | 3 | 22.3.0 |
| 36009194 | In Health Check feature, SCP returns 500 Internal Server Error in HC Response without LCI header when configured Overload Response Profile does not exist | In the health check feature, SCP returned a 500 internal server error in the health check response without an LCI header when the configured overload response profile did not exist. | 3 | 23.3.0 |
| 35976974 | SCP ATS Regression Failure In stage2 Group: G2_PCF_SCP_NRF_CHF_NEF Feature | oc`scp_worker_outstanding_requests` was not pegging correctly, resulting in an ATS failure. | 3 | 23.2.2 |
| 35509384 | SCP has stopped processing NF loads after rollback | The coherence cluster required a restart due to a version change. | 3 | 23.1.2 |
| 35952220 | In Health Check feature,pollingInterval parameter range is not aligned with the requirement | In the Health Check feature, the `PollingInterval` parameter range was not aligned with the requirement. | 3 | 23.3.0 |
| 35952196 | In Health Check feature, requestTimeout parameter range is not aligned with the requirement | In the Health Check feature, the `requestTimeout` parameter range was not aligned with the requirement. | 3 | 23.3.0 |
| 35949184 | Why SCP Health Check feature has been enabled by default? | SCP did not allow the Health Check feature to be disabled, but the CNC Console was not displaying any warnings or notes related to the same. | 3 | 23.2.0 |
| 35936442 | Access token granularity API should not allow duplicate values in mandatory and preferred field values. | Access token granularity API was allowing duplicate values, but this API should not allow duplicate values in mandatory and preferred field values. | 3 | 23.3.0 |
| 36046973 | Unable to validate the scp alternate reroute metric as per the dimensions mentioned in the scp user guide | The dimensions of the `ocscp_metric_http_ar_tx_req_total` metric were documented incorrectly in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*. | 4 | 23.3.1 |

**Table 4-46 (Cont.) SCP 23.4.0 Resolved Bugs**

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 36012996 | ocscp_authority is missing in ocscp_metric_http_tx_req_total and ocscp_metric_http_tx_res_total when ocscp message type is service specific Request | The ocscp_authority dimension was missing in `ocscp_metric_http_tx_req_total` and `ocscp_metric_http_tx_res_total` metrics. | 4 | 23.3.0 |
| 36004773 | SCP syntax errors for SNMP trap MIB definition | Syntax errors were identified in the SCP MIB definition. | 4 | 23.2.0 |
| 35962427 | ocscp_notification_request_total- description is not clear on user guide. | The description of the `ocscp_notification_request_total metric` did not specify the scenario for which it was pegged. | 4 | 23.3.0 |
| 35962359 | SCP is not indicating the consumer details on metrics for service level notification traffic. | SCP did not indicate consumer details, such as `ocscp_consumer_host`, `ocscp_consumer_nf_instance_id`, and `ocscp_consumer_nf_type`, for a few metrics for service level notification traffic. | 4 | 23.3.0 |
| 35900879 | SCP generated 503 is incorrectly mapped IAW 3GPP TS 29.500 version 16.7.0 Release 16 - causing clients to mark SCP as congested and blacklists | Error 503 generated by SCP for connection or timeout failure was not aligned with specifications. | 3 | 23.2.0 |
| 35893481 | SCP shows same dimension multiple times in metrics | Dimensions such as `scp_fqdn` were repeated in some metrics multiple times. | 3 | 23.3.0 |
| 35890052 | SCP Helm chart does not pass Helm Strict Linting Due To Duplicate Entries | There were some duplicate key value pairs in SCP Helm charts, resulting in Helm strict linting test failure. | 3 | 22.3.2 |
| 35865180 | SCP accepts and establishes TLV v1.3 connection when TLSv1.3 is not officially supported | SCP accepted and established a TLS v1.3 connection when TLS v1.3 was not officially supported. | 3 | 23.2.1 |
| 35850549 | SCP was sending 503 error on TX response for Nausf service requests | SCP was sending a 503 error on the TX response for Nausf service requests. | 3 | 23.2.2 |
| 35848570 | SCP ASM config file service entry hosts definition | Support for defining an array of hosts and IP addresses for a service entry was missing in the ASM configuration file. | 3 | 23.2.2 |
| 35657464 | In Oauth2 Feature, Access token Request is getting processed even if requesterInfo is conifgured as CCA header alone and the request does not have CCA header. | In the Oauth2 feature, access token requests were getting processed even if `requesterInfo` was configured as a CCA header alone and the request did not have a CCA header. | 3 | 23.2.0 |

**Table 4-46 (Cont.) SCP 23.4.0 Resolved Bugs**

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 35924127 | User Guide's NRF Configuration section has to be realigned, and the information about the current implementation needs to be updated | In the SCP User Guide, the NRF Configuration sub section was documented under the OAuth Configuration section. | 4 | 23.3.0 |
| 35902551 | Some Attributes are missing in "ocscp_metric_5gsbi_total" Metrics as per User Guide. | Some dimensions of the `ocscp_metric_5gsbi_total` metric were missing from *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*. | 4 | 23.3.0 |
| 35874363 | Upgrade Status section is missing in User Guide | The CNC Console procedure to check the upgrade status of SCP was missing from the *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide.* | 4 | 23.3.0 |
| 35868634 | OC Config examples incorrect | Many examples provided for the `outlierDetection` configuration in the SCP REST API Guide incorrectly showed the value of the interval parameter as less than the value of the `baseEjectionTime` parameter. | 4 | 23.3.0 |
| 35839848 | SCP NFProfileValidator does not print details about why SCP failed the validation | SCP Notification microservice logs were not providing details about failures for profile validation. | 3 | 23.2.0 |
| 35798976 | Need to exclude NRF traffic from Ingress Request rate metrics in default dashboard | SCP dashboard was showing internal traffic as well as the ingress request rate panel. | 4 | 23.3.0 |
| 35798552 | Ocscp-test pod is not getting deleted post helm test | While testing the deployed or upgraded SCP pods, when the pods were installed, they were not removed after the Helm test was performed. | 4 | 23.3.0 |
| 35739879 | ATS user-guide: dbtier pod name listed at table 3-22 are different from current dbtier pod name | In the ATS 23.2.0 User Guide, the cnDBTier pod name was different from the current cnDBTier pod name. | 4 | 23.2.0 |
| 35610819 | Update SCP Routing Options using CLI command | The patch for the routing options update was not working. | 4 | 23.1.1 |

**Note:**

Resolved bugs from 23.2.2 have been forward ported to release 23.4.0.

**Table 4-47 SCP ATS 23.4.0 Resolved Bugs**

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 35896292 | SCP ATS Error in SCP_Circuit_Breaking_Config_API feature | An enhancement to the Circuit Breaking feature file was needed to set the values in the test case correctly. | 3 | 23.3.0 |
| 35753982 | SCP ATS : Unusual behavior during ATS config parameter export | SCP ATS was not setting configuration parameter values correctly when an additional incorrect parameter was added to the list. | 4 | 23.2.2 |

## 4.2.12 SEPP Resolved Bugs

**Table 4-48 SEPP 23.4.2 Resolved Bugs**

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 36674519 | n32fFQDN is required even when seppFqdn is the same | The details for port segregation feature related to n32fFqdn and n32fport were missing from the SEPP documents. | 3 | 23.4.0 |
| 36710549 | Message copy SSL feature parameters not present | The steps to use SSL protocol for message copy were missing from the *Security Edge Protection Proxy Installation, Upgrade, and FaultRecovery Guide*. | 4 | 23.2.1 |

**SEPP 23.4.1 Resolved Bugs**

SEPP 23.4.1 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    SEPP 23.4.0 Resolved Bugs

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 35982232 | SEPP 23.3.0 Rollback to 23.2.0 fails when --wait option is used in helm upgrade command | SEPP 23.3.0 rollback to 23.2.0 failed when the --*wait* option was used in the Helm upgrade command.<br>This issue does not apply for<br>• Upgrade to 23.4.0 through CDCS.<br>• Rollback from future release to SEPP 23.4.0. | 2 | 23.3.0 |
| 35764279 | Upgrade/Rollback for Performance pod failing with CDCS | When performing an upgrade from the source release to SEPP v23.3.0 (Perf-info = 23.3.1), the performance pod behaved randomly.<br>• In some cases, the pod won't come up and after 11 retires, and goes into a crash loopback state.<br>• In some cases the pod was active after 3-4 retries due to the --*wait* parameter added by CDCS when Helm upgrade or rollback is run through CDCS pipeline. This wait parameter forces the steps to be run in a serialized manner which in turn raises a deadlock condition. | 2 | 23.3.0 |
| 35978177 | ATS 23.2.1 for SEPP: Missing Installation details | The installation details were missing in the *Oracle Communications Cloud Native Core, Automated Test Suite User Guide*. | 3 | 23.2.1 |
| 35978102 | OCSEPP 23.2.1 Missing Installation details | The installation details were missing in the *Oracle Communications Cloud Native Core, Automated Test Suite User Guide*. | 3 | 23.2.1 |

**Table 4-49 (Cont.) SEPP 23.4.0 Resolved Bugs**

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 35964923 | SEPP User Guide has outdated examples of CNCC SEPP GUI for Topology Hiding Header and Body tables, causing confusion | SEPP User Guide examples for both Header and Body Topology Hiding tables reflected the older software versions and were outdated. | 3 | 23.2.0 |
| 35941197 | SEPP Install Guide states service.loadBalancer.addressPool is mandatory but is ignored in SEPP deployment and annotations are required but not delineated in the guide | Helm chart ignored the duplicate service keys in custom_values.yaml file. The first service key that contains the `service.loadBalancer.addressPool` was ignored and the second service key was picked up. | 3 | 23.1.3 |
| 35767064 | Rollback failed from 23.3.0 to lower versions with error : no ConfigMap with the name "rss-ratelimit-map" found. | SEPP Rollback from 23.3.0 to the earlier releases (23.1.x and 23.2.x) failed with the following Error: "no ConfigMap" with the name "rss-ratelimit-map".<br>This was a Helm issue, where `configMap` was already present but Helm treated it as it was not present, hence resulting in an error. | 3 | 23.3.0 |
| 35614617 | cn32f and pn32f log level changing from debug to error once the pod is restarted | cn32f-svc and pn32f-svc log levels were reset to old values when the pod was restarted. This was due to the updated values not getting updated in the table. | 3 | 23.2.0 |

Table 4-49 (Cont.) SEPP 23.4.0 Resolved Bugs

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 35767215 | SEPP upgrade fails when executed for second time after performing rollback | When the upgrade was performed to SEPP Release 23.3.0 more than once, after performing a rollback, the upgrade failed with the following error: `Error: UPGRADE FAILED: rendered manifests contain a resource that already exists. Unable to continue with update: ConfigMap "egress-ratelimit-map" in namespace "yash-upgrade" exists and cannot be imported into the current release: invalid ownership metadata; label validation error: missing key "app.kubernetes.io/managed-by": must be set to "Helm"; annotation validation error: missing key "meta.helm.sh/release-name": must be set to "ocsepp-release"; annotation validation error: missing key "meta.helm.sh/release-namespace": must be set to "yash-upgrade"` | 3 | 23.3.0 |
| 35744748 | Coherence service restarting one/twice during installation | The coherence service was restarting during the installation. | 3 | 23.3.0 |
| 35083520 | SEPP-PERF: Clearance issue for alert SEPPN32fTopologyBodyOperationFailureAlert | Some of the alerts were not cleared after a performance traffic stop for *SEPPN32fTopologyBodyOperationFailure* alert and *SEPPPodMemoryUsage* alert. | 3 | 22.4.0 |

**Table 4-49 (Cont.) SEPP 23.4.0 Resolved Bugs**

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 36061888 | Section 3.24 "SEPP also subscribes for UDR profile change in NRF." needs to be updated | The Cat-3 Previous Location Check feature in the SEPP User Guide must be updated. With the changes in SEPP 23.3.x, SEPP does not subscribe to UDR status change in NRF. Thus, this section needs to be updated accordingly. | 4 | 23.3.1 |
| 35976526 | Request with 4 digit mcc in apiRoot header is forwarded to psepp | The header side validation was not present at the sender SEPP. Thus, even if the incorrect mcc and mnc values were given in `3gpp-Sbi-Target-Apiroot`, the `apiRoot` header was forwarded to psepp. | 4 | 23.3.1 |
| 35948268 | Remove duplicate params from alert SEPPPn32fSORTimeoutFailureAlert | In some alerts, there were duplicate attributes present, such as `appname` and `app` and `nfInstanceId` and `nf_instance_id`. | 4 | 23.3.1 |
| 35925831 | Remove duplicate attributes from alerts SEPPN32fNetworkIDValidationHeaderFailureAlert and SEPPN32fNetworkIDValidationBodyIEFailureAlert | In some alerts, there were duplicate attributes present, such as `appname` and `app` and `nfInstanceId` and `nf_instance_id`. | 4 | 23.3.0 |
| 35912471 | For mediation, default error title should be configured | In the mediation error configuration, under the title, error title must be present by default.When the user was given the title with the feature as false for the first time, the error title was not saved until the user set the feature as true. | 4 | 23.3.0 |
| 35912395 | Correct parameter name sorTriggerRuleListName in SEPP REST API guide | The parameter name `TriggerRuleListName` was wrong in the *SOR section* of the *Oracle Communications Cloud Native Core, Security Edge Protection Proxy REST Specification Guide*. | 4 | 23.3.0 |

**Table 4-49 (Cont.) SEPP 23.4.0 Resolved Bugs**

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 35502633 | Section 6.4 Cleaning up Databases; The list of tables needs to be updated | The table list in the Cleaning up Database section in the *Oracle Communications Cloud Native Core, Security Edge Protection Proxy Installation, Upgrade, and Fault Recovery Guide* was as per the old release. | 4 | 23.2.0 |
| 35377315 | Data missing for attributes source and nfinstanceid for SEPPPn32fSORFailure Alert | In the `SEPPPn32fSORFailureAlertPercentAbove50` alert, the source and `nfinstanceid` parameters were not displaying any data. | 4 | 23.1.1 |
| 35248911 | SCM: Response code needs to be corrected when user tries to delete Network ID validation list associated with remote SEPP set | If the user tried to delete the Network ID validation list associated with the Remote SEPP set, error 401 was displayed.<br>*"Error message summary*<br>*[Error Code: 400] - Bad Request - 401 UNAUTHORIZED Please update Network ID Validation List in remote partner set before deleting"* | 4 | 23.1.0 |
| 35940491 | SEPP 23.2.1 CAT2 header Regex not being considered for RURI | CAT-2 Header: The testing showed that it was working normally, that is, if the REGEX is incorrect the CAT-2 feature will be skipped and the SBI request will be passed to the pSEPP.<br>CAT-2 Body: The testing showed that the cSEPP failed to send the SBI request if the REGEX was incorrect and the CAT-2 feature will always be triggered no matter what is the value of the Body IE. | 4 | 23.2.1 |

**Note:**

Resolved bugs from 23.3.x have been forward ported to Release 23.4.0.

## 4.2.13 UDR Resolved Bugs

**Table 4-50 UDR 23.4.2 Resolved Bugs**

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 36617874 | 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 |
| 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 |
| 36682966 | EgressGW http2.remote_reset | "http2.remote_reset" was observed in Egress Gateway logs. | 2 | 23.2.12 |
| 36660374 | Egressgateway buffer memory leak issue and alert missing | Alert was missing when there was Egress Gateway buffer memory leak. | 3 | 23.4.0 |

**Table 4-51 UDR 23.4.1 Resolved Bugs**

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 36447069 | SLF 23.4.0 Conflict Resolution Feature sql file missing in SLF CSAR Package | The SQL files for conflict resolution feature was missing in SLF CSAR package. | 3 | 23.4.1 |
| 36373506 | OCSLF 23.4.0 is not providing "application_layer_protocol_negotiation (16)" ALPN TLS extension in Server Hello message | OCSLF 23.4.0 was not providing Application Layer Protocol Negotiation (ALPN) (16)" Transport Layer Security (TLS) extension in server hello message. | 3 | 23.4.0 |
| 36373494 | OCEIR 23.4.0 is not providing "application_layer_protocol_negotiation (16)" ALPN TLS extension in Server Hello message | OCEIR 23.4.0 was not providing Application Layer Protocol Negotiation (ALPN) (16)" Transport Layer Security (TLS) extension in server hello message. | 3 | 23.4.0 |

Table 4-52    UDR ATS 23.4.2 Resolved Bugs

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 36318088 | Service account creation issue for STUB installation. | STUB installation was creating a service account even though the create value was set as false. | 3 | 23.3.2 |

Table 4-53    UDR ATS 23.4.1 Resolved Bugs

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 36179774 | Service account creation issue for STUB installation in SLF 23.3.1 | STUB installation was creating a service account even though the create value was set as false. | 2 | 23.3.1 |
| 36200825 | SLF ATS test case Subscriber export failure | Multiple test scenarios failed for subscriber export tool. | 3 | 23.3.1 |
| 36162973 | ATS installation failure in PI-D 23.4.0 with static port | ATS installation was failed for 23.4.0 UDR release. | 3 | 23.4.0 |

Table 4-54    UDR 23.4.0 Resolved Bugs

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 35944484 | UserData is incorrect when state entity is deleted in UDR | User Data was incorrect when the state entity was deleted in UDR. | 2 | 23.3.1 |
| 35730602 | PROVGW - In Initial Provisioning, timeout got increased due to latency got increased in a setup | Latency was increased in the initial provisioning due to which the timeout was also increased. | 2 | 23.1.2 |
| 36056995 | UDR Not sending notifications to PCF for SM Data Updates with DB Conflict Resolution feature | UDR was not sending notification to Policy Control Function (PCF) for sm-data updates when database conflict resolution feature was enabled. | 2 | 23.3.1 |
| 35762463 | VSA PUT not merging the subscriber keys when ondemand enabled | Vendor Specific Attribute (VSA) PUT operation was not merging with the subscriber keys when on-demand migration was enabled. | 3 | 23.3.0 |
| 35546979 | SLF - In NF scoring feature, Scoring type parameter in Custom criteria are accepting values other than ratio and weightage | The NF scoring type was accepting values other than ratio and weightage. | 3 | 23.2.0 |

Table 4-54    (Cont.) UDR 23.4.0 Resolved Bugs

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 35547132 | SLF - In NF scoring feature App Info is not periodically fetching the NF score as per default timer | Network Function (NF) score calculation logs were not refreshed periodically as per the default time. | 3 | 23.2.0 |
| 34745401 | User Agent Header is present in UDR EGW messages even when configuration flag is set to false | User-Agent header was added by default in the Egress Gateway messages even when the configuration flag was set to false. | 3 | 22.3.1 |
| 35948090 | Provisioning PUT of subscriber is not validating the Schema | Schema was not getting validated for provisioning PUT of subscribers. | 3 | 23.3.1 |
| 35944773 | UDR is sending 5105 in RC instead of Experimental RC | UDR was sending 5105 in Result Code instead of experimental Result Code. | 3 | 23.3.0 |
| 35933575 | Lab: ME SLF ServiceMesh 23.2.0 Install failure | SLF service mesh installation for 23.2.0 release was failed due to SLF service mesh yaml file error. | 3 | 23.2.0 |
| 35911917 | UDR ATS 23.3 - Regression pipeline failing with Multiple Errors | Regression pipeline was failing with multiple errors for UDR ATS 23.2.0. | 3 | 23.3.0 |
| 35648713 | 0.01% Traffic Loss Observed after EIR and CNDB upgrade in site1 for 2 site GR setup | When Equipment Identity Register (EIR) and cnDBTier was upgraded on Site 1 for two site georeplication stepup there was a traffic loss of 0.0.1%. | 3 | 23.2.0 |
| 35997091 | EGW is not retrying to SCP is 400 Bad Request is received with cause as null and "ignoreCauseIfMissing":true | When sending GET request, UDR was sending 400 Bad Request error response with cause as null. | 3 | 23.3.0 |
| 36069583 | DB Auditor Service throws error during extid key audit in exception table | Database auditor service was throwing an error during extid key audit in exception table. | 3 | 23.3.1 |
| 35869726 | Unable to provision subscribers using CNCC GUI after enabling network policy feature | Subscribers was not provisioned through CNC Console when network policy feature was enabled. | 3 | 23.3.0 |

**Table 4-54 (Cont.) UDR 23.4.0 Resolved Bugs**

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 35992916 | SLF- Overload configuration api URL and its payload in rest document is not updated. | URL and payload was not updated in Configuration APIs for Overload Handling section of the UDR REST API guide. | 3 | 23.3.1 |
| 35948175 | Subscriber tracing -> Unnecessary Extra log for Delete Request | Unnecessary logs were found for delete request. | 4 | 23.3.1 |
| 36071642 | File is not getting transferred (sftp) to remote server when network policy is enabled | Files were not getting transferred to remote server when network policy feature was enabled. | 4 | 23.3.1 |
| 36075830 | File is not getting imported from remote server to pvc when network policy is enabled | Files were not getting imported from remote server to PVC when network policy feature was enabled. | 4 | 23.3.1 |
| 36079114 | DB Auditor Service Metrics Documentation not available in UDR 23.3.1 User Guide | Auditor service metric was not added in 23.3.1 UDR User Guide. | 4 | 23.3.1 |

> **Note:**
>
> Resolved bugs from 23.1.2 have been forward ported to Release 23.4.0.

# 4.2.14 Common Services Resolved Bugs

## 4.2.14.1 Alternate Route Service Resolved Bugs

**Release 23.4.0**

There are no resolved bugs in this release.

## 4.2.14.2 App-Info Resolved Bugs

**Release 23.4.0**

There are no resolved bugs in this release.

## 4.2.14.3 ASM Configuration Resolved Bugs

**Release 23.4.0**

There are no resolved bugs in this release.

### 4.2.14.4 ATS Resolved Bugs

**Table 4-55 ATS 23.4.0 Resolved Bugs**

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 35952185 | ATS: GUI with https (TLS1.2) in ASM is not working. | ATS GUI was not accessible in ASM environments when ATS GUI was HTTPS enabled. | 2 | 23.3.0 |
| 35948863 | Test case count is being displayed wrong on the GUI | The Support for Test Case Mapping and Count feature was not displaying the features and related testcases properly. | 3 | 23.3.0 |
| 35522301 | Unable to set reruns to zero | The option to set the rerun count in parallel testcase execution to zero was not available. | 3 | 23.2.0 |
|  | Make Overall Feature Files Division only display .feature files | The feature files displayed in the overall and stages or groups feature file division sections included files other than “.feature” files. | 4 | 23.3.0 |

### 4.2.14.5 Debug Tool Resolved Bugs

**Release 23.4.0**

There are no resolved bugs in this release.

### 4.2.14.6 Egress Gateway Resolved Bugs

**Release 23.4.x**

**Table 4-56 Egress Gateway 23.4.x Resolved Bugs**

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 35812710 | [NRF-APIGW] SCP monitoring via SCP Health APIs Fails on HTTPS - ERROR Exception frame_size_error/ invalid_frame_length | After the SCP Health Check API feature was configured, the health checks failed, and Egress Gateway logs displayed the following error: frame_size_error/ invalid_frame_length. This issue occurred for all peer SCPs in peer configurations. | 2 | 23.2.4 |

**Table 4-56 (Cont.) Egress Gateway 23.4.x Resolved Bugs**

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 35998237 | [NRF-APIGW] CCA Feature- Ingressgateway isn't able to read caroot.cer from secrets even when cca feature is enabled for accesstoken microservice | After enabling the CCA feature for accesstoken microservice by setting the value to true in the NRF custom.yaml file, it was observed that Ingress Gateway was unable to read caroot.cer for validating the incoming requests. | 2 | 23.4.0 |
| 35953344 | [PCF-APIGW] EGW is not considering routes configured in routesConfig other than 1st routes. | Egress Gateway considered only the first route from routesConfig and selected the correct peer for the request, which matched with the first route. For other requests that considered other routes, peer selection did not happen, and these requests were considered as direct communication requests and sent to the wrong peers. | 2 | 23.2.10 |
| 35959338 | [BSF-APIGW] BSF provide peer health info as healthy even after SBI routing feature is disable[Support for SCP Health API using HTTP2 OPTIONS] | BSF provided peer health information as healthy even after the SBI routing feature was disabled. | 2 | 23.2.0 |
| 35895301 | [SEPP-APIGW] Enabling Open Telemetry with Spring Boot 3.1.3, GW goes into Crash loop Back off state | When OpenTelemetry was enabled in Policy with Gateway 23.4.0, the Gateway pods went into the `CrashLoopBackOff` state. | 2 | 23.4.0 |
| 35831207 | [NRF-APIGW] Significant traffic drop observed during 23.2.8 to 23.1.11 rollback at egw with "shutdown in progress error". Service stabilizes post rollback | The traffic reduced while rolling back Egress Gateway from 23.2.8 to 23.1.11. | 2 | 23.1.11 |
| 35574383 | [SEPP-APIGW] DNS SRV Support- Cache does not refresh once TTL in DNS SRV Entry expires. Forced restart of svc is required for changes to reflect | Cache did not refresh when the TTL in the DNS SRV entry expired. A forced restart of svc (plmn egw and alt svc) was performed for changes to take effect. | 2 | 23.2.3 |

**Table 4-56 (Cont.) Egress Gateway 23.4.x Resolved Bugs**

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 35685511 | [SEPP-APIGW] For Rate Limiting enabled, ERROR log is printed for each discarded request. | When the request was rejected by Rate Limiting (Global, Route, and so on) implemented by Ingress Gateway, an ERROR level log was generated for every discarded message due to which a large number of logs were generated. | 3 | 23.2.0 |
| 35889742 | [SEPP-APIGW] DNS SRV Support- While Re-routing to secondary peer error-reason from primary peer is also printed | It was observed in Egress Gateway 23.4.0, while rerouting to the secondary peer, the error reason from the primary peer was also getting printed. | 3 | 23.4.0 |
| 35667159 | [NRF-APIGW] NRF- aud claim validation {PCF,NRF} failed in CCA header for feature - CCA Header Validation | The aud claim sent in the CCA header with value "aud": ["PCF","NRF"], was rejected with the following error message "status":403,"detail":"aud claim validation failed". | 3 | 23.2.0 |
| 35722575 | [NRF-APIGW]: metrics are not getting pegged in case of multiple root certificate in ocingress-secret for feature - CCA Header Validation | The NRF alert or metric was not populating when multiple root certificates were present in ocingress-secret for the CCA header validation feature. | 3 | 23.2.0 |
| 35959341 | [PCF-APIGW] sbiRouting_cause_based_validation_failure with "cause": "invalid cause path" metrics is not getting incremented | The `oc_egressgateway_sbiRouting_cause_based_validation_failure` metric with "cause": "invalid cause path" did not get incremented. | 3 | 23.2.6 |
| 35750717 | [UDR-APIGW] OpenTelemetry : ProvGW Egress Gateway is not propagating the Trace ID to UDR Ingress Gateway | ProvGW Egress Gateway was not propagating the Trace ID to UDR Ingress Gateway. | 3 | 23.3.3 |
| 35682384 | [NRF-APIGW]: CCA watcher is not running in every 10 min | In NRF, while editing ocingress-secret to add or modify the root certificate, it was not working for the CCA header validation feature. | 3 | 23.2.0 |
| 35599539 | [CONSOLE-APIGW] CNCC: Bearer Token printed on logs | The CNC Console bearer token was printed on logs. | 3 | 22.4.6 |

**Table 4-56 (Cont.) Egress Gateway 23.4.x Resolved Bugs**

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 35842840 | [NRF-APIGW] Egress Gateway is returning different responses based on httpsTargetOnly and httpRuriOnly flags value | When SBI routing and peer monitoring were enabled and all the configured peers were unhealthy, Egress Gateway returned different responses to the back-end microservice based on the values of httpsTargetOnly and httpRuriOnly parameters. | 3 | 23.2.8 |
| 35850726 | [NRF-APIGW] Egress Gateway peer available count metric is -1 for all pods except one | When an NRF was deployed with multiple Egress Gateway pods and SCP peer monitoring was enabled, only one of the Egress Gateway pods pegged the `oc_egressgateway_peer_available_count` metric. All other Egress Gateway pods showed the metric as -1. | 3 | 23.3.4 |
| 35781931 | [SEPP-APIGW] While updating to spring boot 3.1.2 , observing CCACertUtil exception in GW logs | While updating to Spring Boot 3.1.2, CCACertUtil exception was observed in the Gateway logs. | 4 | 23.3.0 |

## 4.2.14.7 Ingress Gateway Resolved Bugs

**Release 23.4.x**

**Table 4-57 Ingress Gateway 23.4.x Resolved Bugs**

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 35914058 | [NRF-APIGW] Pending Message count metric is showing 10x higher values compared to IGW 23.3.4 | While performing NRF benchmarking with Ingress Gateway 23.3.5 and the pod protection feature was enabled with CPU and pending message count, the pending message count reported at Ingress Gateway was 10 times higher. Each pod displayed a pending message count of around 1500. | 2 | 23.3.5 |

**Table 4-57 (Cont.) Ingress Gateway 23.4.x Resolved Bugs**

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 35809111 | [NSSF-APIGW] Incorrect behaviour when errorcodeseriesid is not configured for server header | When `errorcodeseriesId` was not configured at global level and route level, server header was not getting added to any error response. | 2 | 23.3.4 |
| 35795813 | [PCF-APIGW] IGW svc_pending_count increasing updates without decrementing | Overload was triggered in Ingress Gateway in production for PCF-SM. | 2 | 23.1.6 |
| 35983639 | [NRF-APIGW] NRF-Missing mandatory "Subject claim" validation failed with incorrect Error cause "Internal Server Error" for feature - CCA Header Validation | The missing mandatory parameter "Subject claim" validation of the CCA header failed with incorrect error cause "Internal Server Error". | 3 | 23.2.0 |
| 35442983 | [PCF-APIGW] IGW is reporting P_Core & DGW svc as INVALID when SBI OVERLOAD is enabled | In 23.2.0, Ingress Gateway displayed an internal server error for P-Core and DGW invalid value for svcName. | 3 | 23.2.0 |
| 35614486 | [NRF-APIGW] IGW throws IllegalStateException for subsequent streams when Server sends initial GO_AWAY & dns resolution failure even with rolling update | Ingress Gateway displayed `IllegalStateException` for subsequent streams when the server sent an initial GO_AWAY and DNS resolution failure message, even with a rolling update. | 3 | 23.3.0 |
| 34609310 | [SEPP-APIGW] IGW does not generate GO_AWAY during graceful shutdown | Ingress Gateway did not generate GO_AWAY during the graceful shutdown. During the testing of the graceful shutdown, inflight requests were handled by Ingress Gateway. | 3 | 22.1.0 |

## 4.2.14.8 Helm Test Resolved Bugs

**Table 4-58 Helm Test 23.4.0 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 |

### 4.2.14.9 Mediation Resolved Bugs

**Release 23.4.0**

**Table 4-59 Mediation 23.4.0 Resolved Bugs**

| Bug Number | Title | Description | Severity | Found in Release |
|---|---|---|---|---|
| 35727153 | Raising to add service name to the span exporter in telemetry “ as all the other services are adding either the namespace or release name. | While integrating the Mediation service with the latest OpenTelemetry changes, service name was not added to the span exporter in Telemetry. | 3 | 23.3.0 |
| 35768443 | [SEPP] Mediation installation not working with OSO prometheus in ASM mode | The SEPP Mediation installation was not working with OSO Prometheus in ASM mode with the following error: Get "http://10.233.104.205:8091/actuator/prometheus": read tcp 10.233.70.100:51160->10.233.104.205:8091: read: connection reset by peer. | 4 | 23.3.0 |

### 4.2.14.10 Perf-Info Resolved Bugs

**Release 23.4.0**

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 23.4.4 Known Bugs**

There are no known bugs in this release. Known bugs from 23.4.x have been forward ported to release 23.4.4.

**BSF 23.4.2 Known Bugs**

There are no known bugs in this release. Known bugs from 23.4.x have been forward ported to release 23.4.2.

**BSF 23.4.1 Known Bugs**

There are no known bugs in this release. Known bugs from 23.4.0 have been forward ported to release 23.4.1.

**BSF 23.4.0 Known Bugs**

There are no known bugs in this release. Known bugs from 23.1.x and 23.2.x have been forward ported to release 23.4.0.

## 4.3.2 CDCS Known Bugs

**CDCS Release 23.4.0**

**Table 4-60 CDCS 23.4.0 Known Bugs**

| Bug Number | Title | Description | Severity | Found in Release | Customer Impact |
|---|---|---|---|---|---|
| 35753399 | Create Production/Staging Site fails when tried with Bastion Host user other than default | CNE installation using CDCS fails if the user attempts to install CNE using a user name other than the default name mentioned on the Bastion Host. | 3 | 23.2.0 | CNE can still be installed from CDCS, but the user must specify the default user (*cloud-user* for OpenStack and VMware; *admusr* for BareMetal)<br>**Workaround**:<br>No workaround available |

## 4.3.3 CNC Console Known Bugs

**CNC Console 23.4.2**

There are no known bugs in this release.

**CNC Console 23.4.1**

There are no known bugs in this release.

**CNC Console 23.4.0**

There are no known bugs in this release.

## 4.3.4 cnDBTier Known Bugs

**cnDBTier Release 23.4.6**

There are no new known bugs in this release. For the existing known bug, see "cnDBTier 23.4.4 Known Bugs".

**cnDBTier Release 23.4.5**

There are no new known bugs in this release. For the existing known bug, see "cnDBTier 23.4.4 Known Bugs".

### cnDBTier Release 23.4.4

**Table 4-61 cnDBTier 23.4.4 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.<br>**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 23.4.3

**Table 4-62 cnDBTier 23.4.3 Known Bugs**

| Bug Number | Title | Description | Customer Impact | Severity | Found in Release |
|---|---|---|---|---|---|
| 36234344 | With BSF DB 23.2.2.0.0 upgrade, ndbmysqld all pods are restarting frequently. | While performing a cnDBTier upgrade, all `ndbmysqld` pods restart frequently. | mysqld georeplication pods restart when they detect that the binlog injector thread is stalled. However, the automatic action results in a replication channel swicthover and georeplication continues. There is no impact to customer traffic due to the restart of mysqld georeplication.<br>**Workaround:** The system performs the workaround automatically. The system restarts the mysqld geo replication pods when the code monitoring code detects that the bin log injector thread is stalled to prevent impact on the customer traffic. | 2 | 23.2.2 |

Table 4-62 (Cont.) cnDBTier 23.4.3 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 in some of the pods. | Application pods with old password may not be able to connect to cnDBTier database. The connection depends on the mysqld pod that is used to attempt the connection. If the mysqld pod is one of the affected pods, then the connection fails.<br>**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 23.4.2

There are no known bugs in this release.

### cnDBTier Release 23.4.1

There are no known bugs in this release.

### cnDBTier Release 23.4.0

There are no known bugs in this release.

## 4.3.5 CNE Known Bugs

**Table 4-63 CNE 23.4.6 Known Bugs**

| Bug Number | Title | Description | Customer Impact | Severity | Found in Release |
|---|---|---|---|---|---|
| 6740199 | 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 installation hangs on the X9-2 server. When booted with OL9.x ISO UEK, 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.<br>**Workaround:**<br>Perform one of the following workarounds:<br>• Use x8-2 servers.<br>• Use CNE 23.3.x or older version on X9-2 servers. | 2 | 23.4.1 |

Table 4-63 (Cont.) CNE 23.4.6 Known Bugs

| Bug Number | Title | Description | Customer Impact | Severity | Found in Release |
|---|---|---|---|---|---|
| 36869572 | Kyverno timeout leads to failure in CNE upgrade | When performing an CNE upgrade, Kyverno times out intermittently to enforce policies in cluster. This causes the cluster upgrade to fail. | Intermittent failures in CNE upgrade.<br>**Workaround:**<br>Resume the upgrade and rerun the common services upgrade. Perform this step as many times as required, until it succeeds and upgrades all the common services properly. For more information about CNE upgrade, see *Oracle Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide*. | 3 | 23.4.1 |

**Table 4-64 CNE 23.4.4 Known Bugs**

| Bug Number | Title | Description | Customer Impact | Severity | Found in Release |
|---|---|---|---|---|---|
| 36059773 | OCCNE Remove Worker Node is failing due to multiple OSD ID | The script to remove a BareMetal worker node fails when performed using CDCS. | The procedure to remove a BareMetal worker node fails, affecting the overall CDCS automation.<br>**Workaround:**<br>• Do not use the script to remove a worker node.<br>• If required, you can remove the worker node manually when the pipeline fails. | 3 | 23.4.0 |

**Table 4-64 (Cont.) CNE 23.4.4 Known Bugs**

| Bug Number | Title | Description | Customer Impact | Severity | Found in Release |
|---|---|---|---|---|---|
| 35426047 | removeWorkerNode.py not targeting node (Openstack) | The maintenance procedure to automatically remove a Kubernetes worker node does not target the specific node that is given as an argument, while calling Terraform. | Running the removal procedure for any node other than the last one causes Terraform to delete the wrong node. However, the correct node is deleted from the Kubernetes node list and LoadBalancer controller configuration.<br>**Workaround:**<br>• Do not use the automated script to remove a worker node.<br>• If the procedure is already run and the cluster is in an unhealthy state, perform the following steps manually to rectify the issue:<br>– Remove the correct targeted node using Terraform.<br>– Remove the other impacted node (last in the list) from | 3 | 23.2.0 |

**Table 4-64 (Cont.) CNE 23.4.4 Known Bugs**

| Bug Number | Title | Description | Customer Impact | Severity | Found in Release |
|---|---|---|---|---|---|
| | | | the LoadBalancer controller and Kubernetes. However, this is a case by case scenario. | | |

**Table 4-65 CNE 23.4.1 Known Bugs**

| Bug Number | Title | Description | Customer Impact | Severity | Found in Release |
|---|---|---|---|---|---|
| 36308260 | KVM no longer accepts 'ol9' as an os-variant, causes bare-metal deploy failure | CNE Bare Metal deployment creates VMs using the KVM os-variant parameter of 'ol9' which is no longer valid in the latest OL9 update of KVM. | Deployment fails when the provision container logic attempts to create the second Bastion VM and Kubernetes control VMs.<br>**Workaround**:<br>Before deployment, add the `os_variant: ol9.0` parameter in the `[occne:vars]` section of the `hosts.ini` inventory file. | 3 | 23.4.1 |

**Table 4-65 (Cont.) CNE 23.4.1 Known Bugs**

| Bug Number | Title | Description | Customer Impact | Severity | Found in Release |
|---|---|---|---|---|---|
| 36068408 | Grafana issues seen in 23.4.0 | Many panels in Grafana Dashboards are not working as the metric expressions used for the channels are deprecated or updated. | Many panels show "No Data" or empty panel while viewing the cluster data using Grafana.<br>**Workaround**:<br>• Ensure that the new dashboards are listed in Grafana folder list.<br>• Update alerts to ensure that the count of data nodes is used from the `"opensearch_data_replicas_count"` variable. | 3 | 23.4.0 |
| 36059773 | OCCNE Remove Worker Node is failing due to multiple OSD ID | The script to remove a BareMetal worker node fails when performed using CDCS. | The procedure to remove a BareMetal worker node fails, affecting the overall CDCS automation.<br>**Worakround**:<br>• Do not use the script to remove a worker node.<br>• If required, you can remove the worker node manually when the pipeline fails. | 3 | 23.4.0 |

**Table 4-65 (Cont.) CNE 23.4.1 Known Bugs**

| Bug Number | Title | Description | Customer Impact | Severity | Found in Release |
|---|---|---|---|---|---|
| 35426047 | removeWorkerNode.py not targeting node (Openstack) | The maintenance procedure to automatically remove a Kubernetes worker node does not target the specific node that is given as an argument, while calling Terraform. | Running the removal procedure for any node other than the last one causes Terraform to delete the wrong node. However, the correct node is deleted from the Kubernetes node list and LoadBalancer controller configuration.<br>**Workaround**:<br>• Do not use the automated script to remove a worker node.<br>• If the procedure is already run and the cluster is in an unhealthy state, perform the following steps manually to rectify the issue:<br>– Remove the correct targeted node using Terraform.<br>– Remove the other impacted node (last in the list) from | 3 | 23.2.0 |

**Table 4-65 (Cont.) CNE 23.4.1 Known Bugs**

| Bug Number | Title | Description | Customer Impact | Severity | Found in Release |
|---|---|---|---|---|---|
| | | | the LoadBalancer controller and Kubernetes. However, this is a case by case scenario. | | |

**Table 4-66 CNE 23.4.0 Known Bugs**

| Bug Number | Title | Description | Customer Impact | Severity | Found in Release |
|---|---|---|---|---|---|
| 36068408 | Grafana issues seen in 23.4.0 | Many panels in Grafana Dashboards are not working as the metric expressions used for the channels are deprecated or updated. | Many panels show "No Data" or empty panel while viewing the cluster data using Grafana.<br>**Workaround**:<br>• Ensure that the new dashboards are listed in Grafana folder list.<br>• Update alerts to ensure that the count of data nodes is used from the "`opensearch_data_replicas_count`" variable. | 3 | 23.4.0 |

**Table 4-66 (Cont.) CNE 23.4.0 Known Bugs**

| Bug Number | Title | Description | Customer Impact | Severity | Found in Release |
|---|---|---|---|---|---|
| 36059773 | OCCNE Remove Worker Node is failing due to multiple OSD ID | The script to remove a BareMetal worker node fails when performed using CDCS. | The procedure to remove a BareMetal worker node fails, affecting the overall CDCS automation.<br>**Worakround**:<br>• Do not use the script to remove a worker node.<br>• If required, you can remove the worker node manually when the pipeline fails. | 3 | 23.4.0 |

**Table 4-66 (Cont.) CNE 23.4.0 Known Bugs**

| Bug Number | Title | Description | Customer Impact | Severity | Found in Release |
|---|---|---|---|---|---|
| 35426047 | removeWorkerNode.py not targeting node (Openstack) | The maintenance procedure to automatically remove a Kubernetes worker node does not target the specific node that is given as an argument, while calling Terraform. | Running the removal procedure for any node other than the last one causes Terraform to delete the wrong node. However, the correct node is deleted from the Kubernetes node list and LoadBalancer controller configuration.<br>**Workaround**:<br>• Do not use the automated script to remove a worker node.<br>• If the procedure is already run and the cluster is in an unhealthy state, perform the following steps manually to rectify the issue:<br>– Remove the correct targeted node using Terraform.<br>– Remove the other impacted node (last in the list) from | 3 | 23.2.0 |

**Table 4-66 (Cont.) CNE 23.4.0 Known Bugs**

| Bug Number | Title | Description | Customer Impact | Severity | Found in Release |
|---|---|---|---|---|---|
| | | | the LoadBalancer controller and Kubernetes. However, this is a case by case scenario. | | |

**OSO Known Bugs**

**OSO 23.4.5 Known Bugs**

There are no known bugs in this release.

**OSO 23.4.4 Known Bugs**

There are no known bugs in this release.

**OSO 23.4.0 Known Bugs**

There are no known bugs in this release.

## 4.3.6 NEF Known Bugs

**NEF 23.4.4 Known Bugs**

There are no known bugs in this release.

**NEF 23.4.3 Known Bugs**

There are no known bugs in this release.

**NEF 23.4.2 Known Bugs**

There are no known bugs in this release.

**NEF 23.4.1 Known Bugs**

There are no known bugs in this release.

**Table 4-67 NEF 23.4.0 Known Bugs**

| Bug Number | Title | Description | Customer Impact | Severity | Found in Release |
|---|---|---|---|---|---|
| 35753399 | Collision of Reference-Number Diameter AVP in Device Trigger create subscription flow | While creating a Device Trigger transaction flow, there is a probability of collision on the Reference-Number Diameter AVP value that leads to 4xx error response. The higher TPS for Device Trigger Create transactions increase the probability of collision. | The device trigger subscriptions are not created intermittently.<br>**Workaround**:<br>Reattempt to create a successful subscription. | 3 | 23.3.0 |
| 35722356 | Getting intermittent BlackListIpException errors in one NEF microservice while inservice upgrade from 23.2.0 to 23.3.0 | While performing an in-service upgrade from NEF 23.2.0 to 23.3.0, an intermittent issue was identified which occurred due to certain conditions. | `BlackListIpException` might be raised for the requests in *fivegc* agent pods that results in service disruption. This is an intermittent issue, which may not occur for all the requests.<br>**Workaround**:<br>Manually remove the *fivegc* agent pod that is printing `BlackListIpException`. | 3 | 23.3.1 |

**Table 4-67 (Cont.) NEF 23.4.0 Known Bugs**

| Bug Number | Title | Description | Customer Impact | Severity | Found in Release |
|---|---|---|---|---|---|
| 35753770 | Getting intermittent BlackListIpException errors in one NEF microservice while inservice rollback from 23.3.0 to 23.1.0 | While performing an in-service rollback from NEF 23.3.0 to 23.1.0, an intermittent issue was identified which occurred due to certain conditions. | `BlackListIpException` might be raised for the requests in *fivegc* agent pods that results in service disruption. This is an intermittent issue which may not occur for all the requests.<br>**Workaround**:<br>Manually remove the *fivegc* agent pod that is printing `BlackListIpException`. | 3 | 23.3.0 |

# 4.3.7 NRF Known Bugs

**NRF 23.4.4 Known Bugs**

There are no new known bugs for this release.

**NRF 23.4.3 Known Bugs**

There are no new known bugs for this release.

**NRF 23.4.2 Known Bugs**

There are no new known bugs for this release. The known bugs from NRF 23.4.0 are applicable for NRF 23.4.2.

**NRF 23.4.1 Known Bugs**

There are no new known bugs for this release. The known bugs from NRF 23.4.0 are applicable for NRF 23.4.1.

**Table 4-68    NRF 23.4.0 Known Bugs**

| Bug Number | Title | Description | Customer Impact | Severity | Found in Release |
|---|---|---|---|---|---|
| 36106804 | Increase in discovery traffic results into 1 to 2 % failure. The failures settles down after a few minutes. | During the 46.5 Performance Run, it is observed that when traffic steps up at a 3K rate, initially failures are seen in Discovery traffic (~1 to 2%). This settles down in 1-2 mins. | Due to sudden spike in Discovery traffic, failure are observed (1 to 2 %) which gets settles down over the period of 1-2 mins.<br>**Workaround**:<br>In case of failure, retry of `nfDiscover` request by consumer results in success. | 3 | 23.4.0 |

**Table 4-68 (Cont.) NRF 23.4.0 Known Bugs**

| Bug Number | Title | Description | Customer Impact | Severity | Found in Release |
|---|---|---|---|---|---|
| 36366551 | During NRF upgrade from 23.3.1 to 23.4.0 restart observed in NRF ingress-gateway with exit code 143 randomly | During NRF Upgrade from 23.3.1 to 23.4.0, sometime it is observed that NRF ingress-gateway pods restarts. The issue happens only when both the Primary and Secondary Coherence Leader pods gets upgraded at the same time during rolling Update. | This can happen randomly, but when happens, the pod comes up automatically after restart. No manual step is required to recover the pod.<br>**Workaround**:<br>In the ingress-gateway section of the NRF custom_values.yaml file, the `rollingUpgdate.maxUnavailable` and `rollingUpdate.maxSurge` needs to set to 5%. This will ensure only one POD of Ingress Gateway updates at a time. However this will increase the overall upgrade time of all the Ingress Gateway pods. | 3 | 23.4.0 |

## 4.3.8 NSSF Known Bugs

**Table 4-69 NSSF 23.4.0 Known Bugs**

| Bug Number | Title | Description | Customer Impact | Severity | Found in Release |
|---|---|---|---|---|---|
| 36075599 | Replication Channel has broken while doing CNDB rollback 23.4.0.rc.2 to 23.3.1 in site2 | The replication channel breaks while doing a rollback of cnDBTier from 23.4.x. to 23.3.x. | Intermittently, during the rollback of cnDBTier from 23.4.x to 23.3.x in georedundant scenario, the replication is going down.<br>**Workaround**:<br>As a workaround, follow the recovery procedure explained in the sections, *"Resolving Georeplication Failure Between cnDBTier Clusters in a Two Site Replication"* and *"Resolving Georeplication Failure Between cnDBTier Clusters in a Three Site Replication"* in *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide* to recover the replication. | 2 | 23.4.0 |
| 36006744 | NSSF responds with 503 instead for 500 in scenatios of internal error | In scenarios of internal error, NSSF responds with error 503 instead of 500. | There is no loss of service.<br>**Workaround**:<br>No workaround available | 3 | 23.2.0 |

**Table 4-69 (Cont.) NSSF 23.4.0 Known Bugs**

| Bug Number | Title | Description | Customer Impact | Severity | Found in Release |
|---|---|---|---|---|---|
| 35927702 | If TAC is already subscribed, and in Subscription-Patch request, the same TAC is added within TAIList, status code 422 is recieved which is not defined in yaml | NSSF is responding with 422 status code instead of 400 when PATCH for a subscription message contains a duplicate (invalid) value. | There is no loss of service.<br>**Workaround**:<br>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. | REST API for configuration of ocpolicymapping has missing validations. | `ocpolicymapping` configuration is accepting invalid values.<br>**Workaround**:<br>Operator can check the configuration and ensure that the values configured are as per documentation. | 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 congested state. | There is a chance of restart if this behavior continues. However, as per the testing, this is intermittent.<br>**Workaround**:<br>No workaround available | 3 | 23.3.0 |
| 35921656 | NSSF should validate the integer pod protection parameter limit. | REST API for configuration of podprotection has missing validations. | `podprotection` configuration is accepting invalid values.<br>**Workaround**:<br>Operator can check the configuration and ensure that the values configured are as per documentation. | 3 | 23.3.0 |

Table 4-69    (Cont.) NSSF 23.4.0 Known Bugs

| Bug Number | Title | Description | Customer Impact | Severity | Found in Release |
|---|---|---|---|---|---|
| 35888411 | Wrong peer health status is coming "DNS SRV Based Selection of SCP in NSSF" | While selecting an alternate SCP, NSSF is not showing a non responsive SCP as unhealthy, which is a wrong behavior. | There is no impact on traffic flow. A non responsive SCP is not being considered for status that is why there is no status.<br>**Workaround**:<br>No workaround available | 3 | 23.3.0 |
| 35794550 | While sending Discovery Request NssfDiscovery sends Data:<Missing> paramater towards NssfEgw | NrfClient is sending an additional packet which is not to be considered by NRF. | There is no loss of service as NRF ignores the additional packet.<br>**Workaround**:<br>No workaround available | 3 | 23.3.0 |
| 35971708 | while pod protection is disabled, OcnssfIngressGateway PodResourceStateMajor 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. However, when the pod protection feature is disabled, NSSF doesn't check the state of the Gateway pod, resulting in metrics not being cleared.<br>**Workaround**:<br>Check the resource state in Prometheus GUI and observe the NSSF microservices load. Also, ensure that there is no overload scenario. | 3 | 23.3.0 |

**Table 4-69 (Cont.) NSSF 23.4.0 Known Bugs**

| Bug Number | Title | Description | Customer Impact | Severity | Found in Release |
|---|---|---|---|---|---|
| 35975971 | "User agent header support" NSSF is not adding User agent header in Registration, patch, Discovery & subscription towards NRF when "overwriteHeader :false " | NSSF fails to add the User Agent Header even though the feature is enabled, specifically when the Override header is set to false towards NRF. | In call flows directed towards NRF with the 'override' header set to false, the 'User-Agent' header will be absent. This absence does not directly impact the traffic.<br>**Workaround**:<br>Set OverRide header as true. | 3 | 23.3.0 |
| 35927764 | NSSF is accepting a TAC with value 0 and then accepting a patch with ADD op on TAC O | NSSF must reject the patch as same TAC must not be accepted with ADD operation. | There is no loss of traffic. NSSF is accepting a PATCH with ADD operation only when TAC is 0, which is rare.<br>**Workaround**:<br>No workaround available | 3 | 23.3.0 |
| 35502848 | Rest API for configuration of PeerMoniteringConfiguration has missing validations. | REST API for configuration of `PeerMoniteringConfiguration`has missing validations. | `PeerMoniteringConfiguration` configuration is accepting invalid value of timeout.<br>**Workaround**:<br>The operator can check the configuration and ensure that the values configured are as per documentation. | 3 | 23.2.0 |

**Table 4-69 (Cont.) NSSF 23.4.0 Known Bugs**

| Bug Number | Title | Description | Customer Impact | Severity | Found in Release |
|---|---|---|---|---|---|
| 35701232 | "422 Bad Request Error Json" even on not giving proper path value in PATCH request | Error detail while responding to an invalid patch request ID is not in sync with the user guide. | There is no impact on traffic as the invalid message is being responded to as an error. However, the issue is in the error detail as it is not as per the user guide.<br>**Workaround**:<br>No workaround available | 3 | 23.2.0 |
| 35796052 | In Service Solution upgrade ASM enabled:2 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 is crossing the threshold of 50ms and going till 237ms for some messages. | There is no loss of service as this does not cause a timeout.<br>**Workaround**:<br>No workaround available | 3 | 23.3.0 |

Table 4-69 (Cont.) NSSF 23.4.0 Known Bugs

| Bug Number | Title | Description | Customer Impact | Severity | Found in Release |
|---|---|---|---|---|---|
| 35966454 | When AMF sends Patch request for adding a slice (EABB25) in subscribed TAC , I am recieving 2 notifications, one without slice EABB25 and then later one with the slice EABB25 in it. | NSSF sends two notifications when Patch request on `NsAvailability` leads to a configuration update. | NSSF sends an additional message (Notification) when a PATCH request on NsAvailabilityData triggers a configuration change. This infrequent occurrence takes place when there is an update in the AMF configuration. Consequently, the impact is minimal, and these notifications from NSSF based on patches are rare occurrences that do not clutter the network.<br>**Workaround**:<br>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. | `errorcodeserieslist` is accepting invalid values.<br>**Workaround**:<br>The operator can check the configuration and ensure that the values configured are as per documentation. | 4 | 23.3.0 |

Table 4-69 (Cont.) NSSF 23.4.0 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. | `routesconfiguration` is accepting invalid values where abatement value is less than onset.<br>**Workaround**:<br>The operator can check the configuration and ensure that the values configured are as per documentation. | 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 Configuration has missing validations. | Overload Level Threshold configuration is accepting invalid values where abatement value is less than onset.<br>**Workaround**:<br>The operator can check the configuration and ensure that the values configured are as per documentation. | 4 | 23.3.0 |

**Table 4-69 (Cont.) NSSF 23.4.0 Known Bugs**

| Bug Number | Title | Description | Customer Impact | Severity | Found in Release |
|---|---|---|---|---|---|
| 35394240 | CandidateAmfList is not added by NSSF when No AMF is sending the ns-availability update request to NSSF | The PLMN level profile serves as the default profile when no other profile applies, determining the AMFs for a UE. However, the operator-configured rule takes precedence over the PLMN level profile, specifying a different set of AMFs.<br>When no AMF sends availability updates for a specific PLMN level profile, it results in no AMF set being mapped to that profile. Consequently, the UE is not able to connect to any AMFs, leading to an inability to access the network. | This scenario represents a rare case. The designed PLMN Level Profile (Default profile) is mapped to an operator-configured rule. No AMF in the network is sending an Availability Update, resulting in no mapping of an AMF set to that profile. Consequently, this creates a situation where no AMF set is linked due to the absence of availability updates.<br>**Workaround**:<br>The operator must configure Rule and Map with a Network Slice profile rather than a default PLMN profile. | 4 | 23.1.0 |
| 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 Tai List and TaiRange List. However, there is a discrepancy in the specification whether both must be supported. Since support exists for each parameter separately, there is no loss of traffic. | There is no loss of traffic.<br>**Workaround**:<br>The operator must configure Rule and Map with a Network Slice profile rather than a default PLMN profile. | 4 | 23.1.0 |

## 4.3.9 OCCM Known Bugs

### OCCM 23.4.3 Known Bugs

There are no known bugs in this release.

### OCCM 23.4.2 Known Bugs

There are no known bugs in this release.

### OCCM 23.4.1 Known Bugs

There are no known bugs in this release.

### OCCM 23.4.0 Known Bugs

There are no known bugs in this release.

## 4.3.10 Policy Known Bugs

### Policy 23.4.6 Known Bugs

There are no known bugs in this release. Known bugs from 23.4.x have been forward ported to release 23.4.6.

**Table 4-70 Policy 23.4.5 Known Bugs**

| Bug Number | Title | Description | Severity | Found In Release | Customer Impact |
|---|---|---|---|---|---|
| 36907476 | DIAMGW TPS is limiting to 8k and Unable to reach 10K TPS | Diameter Gateway is limiting to 8k TPS and is unable to reach 10K TPS. | 3 | 24.1.0 | There is no customer impact.<br>**Workaround**: No workaround available. |
| 36885128 | SM-PCF - 23.2.7 to 23.4.4 upgrade does not retain CM GUI diam-gateway Error Config | In Policy 23.2.7, the Diameter Gateway error is configured in CNC Console. These configurations are not retained when Policy is upgraded to 23.4.4. In Policy 23.4.4, the default configuration for Diameter Gateway service is considered as disabled for each Error State. | 2 | 23.4.4 | There is no customer impact.<br>**Workaround**: No workaround available. |

Table 4-70 (Cont.) Policy 23.4.5 Known Bugs

| Bug Number | Title | Description | Severity | Found In Release | Customer Impact |
|---|---|---|---|---|---|
| 36943463 | Minor Limitations on ExcludeDNN Functionality | The excludeDnn feature has the following limitations:<br>• PRE can trigger SSV Update even if excludeDNN is enabled for PDS.<br>• Cleanup process is sending request to policyds when "excludeDnn" is enabled. | 3 | 23.4.5 | There are limitations on advanced use cases like SSV-Update triggered through Policy and session removal through Session Viewer.<br>**Workaround**: Change the policies to block this on specific DNNs. |
| 36948349 | Subscriber Activity Logging for IPv4 and IPv6 are causing DIAMETER_UNABLE_TO_COMPLY in SLR | Session Limiting Request (SLR)s are responded with *DIAMETER_UNABLE_TO_COMPLY* when the IPv4/IPv6 based Subscriber Activity Logging (SAL) is enabled. SUPI/GPSI based SAL works for Sy interface. | 3 | 24.3.0 | IPv4/IPv6 address based SAL does not work for Sy interface and corresponding Sy message fails with 5012.<br>**Workaround**: IPv4/IPv6 address can be used for the SAL. |

### Policy 23.4.4 Known Bugs

There are no known bugs in this release. Known bugs from 23.4.x have been forward ported to release 23.4.4.

### Policy 23.4.3 Known Bugs

There are no known bugs in this release. Known bugs from 23.4.x have been forward ported to release 23.4.3.

### Policy 23.4.2 Known Bugs

There are no known bugs in this release. Known bugs from 23.4.x have been forward ported to release 23.4.2.

### Policy 23.4.1 Known Bugs

There are no known bugs in this release. Known bugs from 23.4.0 have been forward ported to release 23.4.1.

**Table 4-71 Policy 23.4.0 Known Bugs**

| Bug Number | Title | Description | Customer Impact | Severity | Found in Release |
|---|---|---|---|---|---|
| 35906844 | PCF not retrying for subsequent request PUT:nchf-spendinglimitcontrol/v1/subscriptions/ due to an exception raised | PCF is not retrying for the subsequent request `PUT:nchf-spendinglimitcontrol/v1/subscriptions/` due to an exception. | In case the CHF responds with the empty body, retry will not happen. But if the CHF responds with correct body, then retry will happen based on the retry profile.<br>**Workaround**:<br>No workaround available | 3 | 23.2.4 |
| 36113402 | User_connector : "Observing that Subsequent PATCH requests are not sent to the UDR which was selected for 1st PATCH request with DNS SRV fall back mechanism and that UDR had sent 2xx response to 1st UE PATCH." | Subsequent patch requests are not sent to the UDR which was selected for first patch request with DNS SRV fall back mechanism and that UDR had sent 2xx response to first UE PATCH." | As UDR-1 had failed earlier, and it is still unavailable, PCF may consume an additional retry attempt and additional latency to retry to UDR-2. However, the latency is not a significant concern as PATCH messages are asynchronous to other flows. Also, since UDR-1 and UDR-2 belong to the same set, the data should be synchronized irrespective of which UDR is patched.<br>**Workaround**:<br>No workaround available | 3 | 23.4.0 |

**Table 4-71 (Cont.) Policy 23.4.0 Known Bugs**

| Bug Number | Title | Description | Customer Impact | Severity | Found in Release |
|---|---|---|---|---|---|
| 36113588 | UE N1N2 Unsubscribe Session Retry Not Working | N1N2 unsubscribe message session retry is not working after failure in the first regular attempt when SBI binding header is not present in N1N2 subscribe message response. | When Binding Header is missing in the Subscribe response from AMF, retry of the unsubscribe message will not happen based on the NF set information contained in AMF profile. If DNS SRV is enabled, then retry logic will happen based on the DNS SRV.<br>**Workaround**:<br>No workaround available | 3 | 23.4.0 |
| 36113786 | INDICATION_OF_IP_CAN_CHANGE specific action AVP is being generated by SM even though there is no change in IP CAN TYPE | INDICATION_OF_IP_CAN_CHANGE specific action AVP is being generated by SM when there is no change in IP CAN TYPE. | The UNSUCCESSFUL_RESOURCE_ALLOCATION error occured during Sm Update with ratType/AccessType change.<br>**Workaround**:<br>No workaround available | 3 | 23.3.0 |
| 36113417 | "Fallback to high priority destination" flag is not working in udr-conn | The "Fallback to high priority destination" flag is not working in UDR Connector. | When PCF retries to a lower priority destination NF after a higher priority destination NF fails, the "Fallback to higher priority destination" feature enables an operator to fall back to the higher priority NF after a pre-configured interval of time. The impact is that the signaling will continue with the last successful destination it fails. Once that destination fails, the retry logic will consider the higher priority destination again.<br>**Workaround**:<br>No workaround available | 3 | 23.2.4 |

Table 4-71 (Cont.) Policy 23.4.0 Known Bugs

| Bug Number | Title | Description | Customer Impact | Severity | Found in Release |
|---|---|---|---|---|---|
| 36113424 | User_connector : "Observing that UDR connector is sending subsequent PATCH request to wrong UDR in a scenario where UE GET resulted in 2xx with a 3gpp-Sbi-Target-apiRoot". | UDR connector is sending subsequent PATCH request to wrong UDR in a scenario where UE GET resulted in 2xx with a `3gpp-Sbi-Target-apiRoot`. | As UDR had failed earlier and it is still unavailable, PCF may consume an additional retry attempt and additional latency to retry to another UDR. The latency is not a significant concern as PATCH messages are asynchronous to other flows. Since the UDRs in context belong to the same set or are geo-redundant, the data should be synced irrespective of which UDR is patch-ed.<br>**Workaround**:<br>No workaround available | 3 | 23.4.0 |
| 36113441 | Traffic distribution is not equal in UM svc | Traffic distribution is not equal in UM service. | The minimum and maximum replica counts need to be set to a higher than the calculated number because of the unequal traffic distribution. This is because the mean traffic being processed may not be accurate enough to load a particular UM service pod upto 80% of CPU utilization. It is recommended to keep the CPU utilization to a lower number (fo example, 60%) till this bug it fixed.<br>**Workaround**:<br>A service mesh can offer better traffic distribution. | 3 | 23.4.0 |

**Note:**

Known bugs from 23.1.x and 23.2.x have been forward ported to Release 23.4.0.

## 4.3.11 SCP Known Bugs

### SCP 23.4.3 Known Bugs

There are no known bugs in this release.

### SCP 23.4.2 Known Bugs

There are no known bugs in this release.

### SCP 23.4.1 Known Bugs

There are no known bugs in this release.

**Table 4-72 SCP 23.4.0 Known Bugs**

| Bug Number | Title | Description | Customer Impact | Severity | Found in Release |
|---|---|---|---|---|---|
| 36128794 | Message Copy feature not working post upgrade from 23.3.0 to 23.4.0 | The Message Feed feature is not working after upgrading from 23.3.0 to 23.4.0. | The Message Feed feature does not work if SSL or SASL is enabled towards Oracle Communications Network Analytics Data Director (DD).<br>**Workaround**:<br>Disable SSL or SASL for Message Feed. | 2 | 23.4.0 |

## 4.3.12 SEPP Known Bugs

### SEPP 23.4.2 Release

There are no known bugs in this release.

### SEPP 23.4.1 Known Bugs

SEPP 23.4.1 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 4-73 SEPP 23.4.0 Known Bugs**

| Bug Number | Title | Description | Customer Impact | Severity | Found In Release |
|---|---|---|---|---|---|
| 35036599 | [SEPP-APIGW] Total traffic loss after upgrade when global Ingress rate limiting feature is enabled | The user is facing total traffic failure when upgrading from any SEPP release to 23.4.x, and the rate limit feature is ON. The following exception is noticed after the upgrade and the traffic is fine if the ingress port is restarted.<br>Restart the ingress pod.<br>`Role=SpringframeworkBootLoaderJarLauncher))io.github.bucket4j.BucketConfiguration; class invalid fordeserialization","message":"(Wrapped: Failed request execution forMapDistCache service on Member(Id=2)` | If the Global Rate Limiting feature is enabled, and the traffic is in progress and the upgrade is performed to any release, then after the upgrade, n32-ingress-gateway stops processing the traffic. There will be a total loss.<br>**Workaround**:<br>• If the SBI traffic is in progress during the upgrade, after the upgrade, restart the n32-ingress-gateway. The system will recover and start processing traffic.<br>• Perform an upgrade with the globalRateLimiting set to disabled. | 2 | 22.4.0 |

**Table 4-73 (Cont.) SEPP 23.4.0 Known Bugs**

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

Table 4-73 (Cont.) SEPP 23.4.0 Known Bugs

| Bug Number | Title | Description | Customer Impact | Severity | Found In Release |
|---|---|---|---|---|---|
| 36026779 | EGW restart observed | The Gateway restarts are observed at the advertised capacity of 5000 MPS per POD, and PLMN Ingress gateway starts showing memory issues resulting in restart of the service. The issue requires more investigation and triage. As an interim and temporary measure, by reducing the supported MPS per POD to 3200, the resource profile and Dimensioning sheet will be updated to reflect this degradation. | Overall System throughput has been reduced to 54 K MPS with an increased pod count, and the per pod throughput has been reduced to 3200 MPS from 5000.<br>**Workaround**:<br>No workaround available | 3 | 23.3.0 |
| 36035492 | PLMN IGW restarts due to java.lang.OutOfMemoryError | The Gateway restarts are observed at the advertised capacity of 5000 MPS per POD, this is also observed with DNS SRV feature enabled. The issue requires more investigation and triage. As an interim and temporary measure, reducing the supported MPS per POD to 3200, the resource profile and Dimensioning sheet will be updated to reflect this degradation. | Overall System throughput has been reduced to 54 K MPS with an increased pod count, and the per pod throughput has been reduced to 3200 MPS from 5000.<br>**Workaround**:<br>No workaround available | 3 | 23.4.0 |

Table 4-73 (Cont.) SEPP 23.4.0 Known Bugs

| Bug Number | Title | Description | Customer Impact | Severity | Found In Release |
|---|---|---|---|---|---|
| 35527387 | DNS SRV Support- Loss of SEPP forwarding Traffic at IGW with DNS SRV enabled at high TPS | The Gateway restarts are observed at the advertised capacity of 5000 MPS per POD, the issue requires more investigation and triage. As an interim and temporary measure, reducing the supported MPS per POD to 3200, the resource profile and Dimensioning sheet will be updated to reflect this degradation. | Overall System throughput has been reduced to 54 K MPS with an increased pod count, and the per pod throughput has been reduced to 3200 MPS from 5000.<br>**Workaround**:<br>No workaround available | 3 | 23.2.3 |
| 35898970 | DNS SRV Support- The time taken for cache update is not same TTL value defined in SRV record. | The time taken to update the cache is not the same as the TTL defined in SRV records. Sometimes the cache updates even before TTL Expires and at others, the cache updates later than the TTL.<br>Expectation: The cache must be updated as per TTL, that is, once TTL has expired, if TTL is 60, then the cache must be updated after every 60. | If the priority or weight is changed, it might take a longer time than TTL to get the cache updated and for the changes to reflect in the environment.<br>**Workaround**:<br>After changing the configuration, restart the `n32-egress-gateway` and `alternate-route-svc`. | 3 | 23.4.0 |

**Table 4-73 (Cont.) SEPP 23.4.0 Known Bugs**

| Bug Number | Title | Description | Customer Impact | Severity | Found In Release |
|---|---|---|---|---|---|
| 35919133 | DNS SRV Support-Custom values key "dnsSrvEnabled" does not function as described | Custom values key `dnsSrvEnabled` description mentions its use as a 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. Issue: Even when Flag is made false and the setup is upgraded, the curl reaches core DNS.<br>Scenario: 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 so that the request must not reach core DND. | In the case of virtual FQDN, the query will always go to core DNS.<br>**Workaround**:<br>Do not configure records in core DNS. | 3 | 23.4.0 |
| 35750433 | Incorrect deletion of action set and criteria set | The action set and criteria set can be deleted even though they are associated with routes.<br>The operator needs to put a check on the deletion of the action set and criteria set, once the routes configuration is configured. | retry and reroute mechanism would not work if the action set and criteria set are deleted.<br>**Workaround**:<br>Do not delete the action set and criteria set if they are associated with routes. | 3 | 23.3.3 |

**Table 4-73 (Cont.) SEPP 23.4.0 Known Bugs**

| Bug Number | Title | Description | Customer Impact | Severity | Found In Release |
|---|---|---|---|---|---|
| 36111800 | Generation of Watcher exception logs on IGW/EGW without any traffic | Watcher exceptions are observed in gateway logs when SEPP is installed on OCCNE 23.4.0-rc.1 cluster. | Extra error logs are observed,which might result in filling ephemeral storage.<br>**Workaround**:<br>No workaround available | 3 | 23.4.0 |
| 36071946 | The mediation rule in the draft state can be overwritten if the user creates another mediation rule with the same name | The mediation rule in the draft state can be overwritten if the user creates another mediation rule with the same name. Expected behavior: The user should not be able to overwrite the existing rule. | The rule in the draft state will be overwritten if a new rule with the same name is created by mistake.<br>**Workaround**:<br>There is no workaround available. It is recommended to save the rules that are required in the future in the SAVE state. | 3 | 23.3.0 |
| 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.<br>**Workaround**:<br>No workaround available | 4 | 23.3.0 |
| 34374452 | SEPP-COM-xx-ERROR-0103 was not observed when n32c pods were scaled down | On scaling down pn32c and cn32c pods, if a delete request is run for the configured Remote SEPP, 204 is returned but the entry is not deleted. No error is displayed when a POST request is run and all the pods are scaled down. | There is no customer impact.<br>**Workaround**:<br>Ensure that the pod and the service are up. Run the command and the run will be successful. | 4 | 22.3.0 |

## 4.3.13 UDR Known Bugs

**UDR 23.4.2 Known Bugs**

There are no known bugs in this release.

**UDR 23.4.1 Known Bugs**

There are no known bugs in this release.

**Table 4-74 UDR 23.4.0 Known Bugs**

| Bug Number | Title | Description | Customer Impact | Severity | Found in Release |
|---|---|---|---|---|---|
| 35762491 | Diameter Gateway metric validation for missing avp in SNA and PUA response is getting pegged twice | Metric validation on Diameter Gateway is pegged twice for the missing Attribute Value Pair (AVP). | There is no impact. Metrics need to be ignored for this test case.<br>**Workaround**:<br>No workaround available | 3 | 23.4.0 |
| 36094811 | Migration tool performance issue to read records from 4G UDR at high TPS | There is preformance issue from the migration tool to read records from 4G UDR at high TPS. | The data migration time is increased.<br>**Workaround**:<br>No workaround available | 3 | 23.4.0 |
| 36094553 | Notifications are inconsistently failing to reach server from egressgateway once 503 response is received from the server | Notifications were inconsistently failing to reach server from Egress Gateway, when 503 response was received from the server. | This scenario is not seen in most of the deployments.<br>**Workaround**:<br>No workaround available | 3 | 23.4.0 |

## 4.3.14 Common Services Known Bugs

### 4.3.14.1 Alternate Route Service Known Bugs

**Release 23.4.0**

There are no known bugs in this release.

## 4.3.14.2 App-Info Known Bugs

**Release 23.4.0**

There are no known bugs in this release.

## 4.3.14.3 ASM Configuration Known Bugs

**Release 23.4.0**

There are no known bugs in this release.

## 4.3.14.4 ATS Known Bugs

**Release 23.4.0**

There are no known bugs in this release.

## 4.3.14.5 Debug Tool Known Bugs

**Release 23.4.0**

There are no known bugs in this release.

## 4.3.14.6 Egress Gateway Known Bugs

**Release 23.4.x**

**Table 4-75 Egress Gateway 23.4.x Known Bugs**

| Bug Number | Title | Description | Customer Impact | Severity | Found in Release |
|---|---|---|---|---|---|
| 36047564 | [NRF-APIGW] Egress traffic fails completely after 21K+ | Egress Gateway traffic fails after the traffic exceeds 21K TPS. | Traffic loss and pod restarts may be experienced.<br>**Workaround**:<br>It is recommended to increase sizing capacity of Egress Gateway or Ingress Gateway pods with the maximum load factor to not exceed 1500 TPS per each Gateway pod. | 3 | 23.4.0 |

**Table 4-75 (Cont.) Egress Gateway 23.4.x Known Bugs**

| Bug Number | Title | Description | Customer Impact | Severity | Found in Release |
|---|---|---|---|---|---|
| 36026779 | [SEPP-GW] EGW restart observed | Egress Gateway restarts when the error max local stream count exceeds. | Traffic loss and pod restarts may be experienced.<br>**Workaround**:<br>It is recommended to increase sizing capacity of Egress Gateway or Ingress Gateway pods with the maximum load factor to not exceed 1500 TPS per each Gateway pod. | 3 | 23.4.0 |

## 4.3.14.7 Ingress Gateway Known Bugs

**Table 4-76 Ingress Gateway 23.4.x Known Bugs**

| Bug Number | Title | Description | Customer Impact | Severity | Found in Release |
|---|---|---|---|---|---|
| 36089693 | SPAD_POLICY:[SM Performance] Executing 60K TPS in SM call Model (1:74:1) , IGW has degradation in performace compare to earlier release 23.2.X | During execution and verification of 60K TPS on a single site, performance degradation is observed, and the number of errors and utilization in Ingress Gateway has increased as compared to the previous run. | Traffic loss and pod restarts may be experienced.<br>**Workaround**:<br>It is recommended to increase sizing capacity of Egress Gateway or Ingress Gateway pods with the maximum load factor to not exceed 1500 TPS per each Gateway pod. | 2 | 23.4.1 |

Table 4-76 (Cont.) Ingress Gateway 23.4.x Known Bugs

| Bug Number | Title | Description | Customer Impact | Severity | Found in Release |
|---|---|---|---|---|---|
| 36035492 | [SEPP-GW] PLMN IGW restarts due to java.lang.OutOfMemoryError | `java.lang.OutOfMemoryError` errors are observed on PLMN Ingress Gateway at 2000 TPS. | Traffic loss and pod restarts may be experienced.<br>**Workaround**:<br>It is recommended to increase sizing capacity of Egress Gateway or Ingress Gateway pods with the maximum load factor to not exceed 1500 TPS per each Gateway pod. | 3 | 23.4.0 |
| 35527387 | [SEPP-APIGW] DNS SRV Support- Loss of SEPP forwarding Traffic at IGW with DNS SRV enabled at high TPS | SEPP traffic is reducing at Ingress Gateway when DNS SRV is enabled at high TPS. | High Latency may be experienced above 2100 TPS.<br>**Workaround**:<br>It is recommended to increase sizing capacity of Egress Gateway pods with the maximum load factor to not exceed 2000 TPS per each Gateway pod. | 3 | 23.2.3 |

## 4.3.14.8 Helm Test Known Bugs

**Release 23.4.0**

There are no known bugs in this release.

## 4.3.14.9 Mediation Known Bugs

**Release 23.4.0**

There are no known bugs in this release.

## 4.3.14.10 NRF-Client Known Bugs

**Release 23.4.0**

There are no known bugs in this release.

## 4.3.14.11 Perf-Info Known Bugs

**Perf-Info 23.4.0 Known Bugs**

There are no known bugs in this release.