Oracle® Communications

Cloud Native Core Release Notes

Release 3.24.3

G17550-14

July 2025

Oracle Communications Cloud Native Core Release Notes, Release 3.24.3

G17550-14

Contents

1 Introduction

2 Feature Descriptions

3 Media and Documentation

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 3.24.3 - G17550-14, July 2025

NSSF 24.3.2 Release

Updated the following sections with the details of NSSF release 24.3.2:

- Common Microservices Load Lineup

Release 3.24.3 - G17550-13, July 2025

NSSF 24.3.2 Release

Updated the following sections with the details of NSSF release 24.3.2:

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

Release 3.24.3 - G17550-12, June 2025

CNE 24.3.3 Release

Updated the following sections with the details of CNE release 24.3.3:

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

Release 3.24.3 - G17550-11, May 2025

NSSF 24.3.1 Release

Updated the following sections with the details of NSSF release 24.3.1:

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

Release 3.24.3 - G17550-10, May 2025

SEPP 24.3.2 Release

Updated the following sections with the details of SEPP release 24.3.2:

- Media Pack

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

Release 3.24.3 - G17550-09, March 2025

cnDBTier 24.3.1 Release

Updated the following sections with the details of cnDBTier release 24.3.1:

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

OSO 24.3.1 Release

Removed the updates related to Time Series Database (TSDB) Snapshots feature from the Cloud Native Environment (CNE) section as this feature is not supported in this release.

Release 3.24.3 - G17550-08, February 2025

CNE 24.3.2 Release

Added the following bugs in the CNE Known Bugs section:

- 37564804
- 37552439

Release 3.24.3 - G17550-06, February 2025

SEPP 24.3.1 Release

Updated the following sections with the details of SEPP release 24.3.1:

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

Release 3.24.3 - G17550-05, January 2025

CNE 24.3.2 Release

Updated the following sections with the details of CNE release 24.3.2:

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

OSO 24.3.1 Release

Updated the following sections with the details of OSO release 24.3.1:

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

cnDBTier 24.3.0 Release

Added a bug in the cnDBTier Known Bugs section.

OSO 24.3.0 Release

Updated the Kubernetes version in the Compatibility Matrix section.

Release 3.24.3 - G17550-05, January 2025

SCP 24.3.0 Release

Added a resolved bug in the SCP Resolved Bugs section.

Release 3.24.3 - G17550-04, December 2024

CNE 24.3.0 Release

Added a bug in the CNE Known Bugs section.

Release 3.24.3 - G17550-03, December 2024

CNE 24.3.1 Release

Updated the following sections with the details of CNE release 24.3.1:

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

NRF 24.3.0 Release

Added a note in the NRF Known Bugs section to mention that known bugs from 24.1.x and 24.2.x have been forward ported to Release 24.3.0.

Release 3.24.3 - G17550-02, November 2024

Policy 24.3.0 Release

Updated the following sections with the details of Policy release 24.3.0:

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

Release 3.24.3 - G17550-01, November 2024

ATS 24.3.0 Release

Updated the following sections with the details of ATS release 24.3.0:

- Automated Testing Suite (ATS) Framework

BSF 24.3.0 Release

Updated the following sections with the details of BSF release 24.3.0:

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

CNC Console 24.3.0 Release

Updated the following sections with the details of CNC Console release 24.3.0:

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

cnDBTier 24.3.0 Release

Updated the following sections with the details of cnDBTier release 24.3.0:

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

CNE 24.3.0 Release

Updated the following sections with the details of CNE release 24.3.0:

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

- CNE Known Bugs

OSO 24.3.0 Release

Updated the following sections with the details of OSO release 24.3.0:

- OSO
- Media Pack
- Compatibility Matrix

NRF 24.3.0 Release

Updated the following sections with the details of NRF release 24.3.0:

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

NSSF 24.3.0 Release

Updated the following sections with the details of NSSF release 24.3.0:

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

OCCM 24.3.0 Release

Updated the following sections with the details of OCCM release 24.3.0:

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

OCI Adaptor 24.3.0 Release

Updated the following sections with the details of OCI release 24.3.0:

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

SCP 24.3.0 Release

Updated the following sections with the details of SCP release 24.3.0:

- 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

SEPP 24.3.0 Release

Updated the following sections with the details of SEPP release 24.3.0:

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

UDR 24.3.0 Release

Updated the following sections with the details of UDR release 24.3.0:

- Unified Data Repository (UDR)
- Media Pack
- Compatibility Matrix
- 3GPP Compatibility Matrix
- Common Microservices Load Lineup
- UDR 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 24.3.0:

- ATS Resolved Bugs
- Egress Gateway Resolved Bugs
- Ingress Gateway Resolved Bugs
- NRF-Client Resolved Bugs

Common Services Known Bugs

Updated the following sections with the details of Common Services Known Bugs for release 24.3.0:

- Alternate Route Service Known Bugs
- Egress Gateway Known Bugs
- Ingress Gateway Known Bugs
- NRF-Client 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 3.24.3.

2.1 Automated Testing Suite (ATS) Framework

Release 24.3.0

Oracle Communications Cloud Native Core, Automated Test Suite (ATS) framework 24.3.0 includes the following enhancements:

- **ATS Custom Abort**: This feature allows you to gracefully abort the ongoing build directly from the Graphical User Interface (GUI). For more information, see *"ATS Custom Abort"* section in *Oracle Communications Cloud Native Core, Automated Test Suite Guide*.
- **ATS Health Check**: This feature allows you to evaluate the health of the ATS deployment by performing several checks after installation to ensure that all components are functioning properly. For more information, see *"ATS Health Check"* section in *Oracle Communications Cloud Native Core, Automated Test Suite Guide*.

2.2 Binding Support Function (BSF)

Release 24.3.0

Oracle Communications Cloud Native Core, Binding Support Function (BSF) 24.3.0 includes the following enhancements:

- **Logging Support for Error Response in BSF**: BSF sends error responses to consumer NFs due to some exceptions, such as signaling, validations, and internal errors. These error responses have payloads containing the problem title, status, details, and cause of the error that are used to investigate the error. BSF has been enhanced to support logs for the error responses. For more information, see *"Logging Support for Error Response in BSF"* section in *Oracle Communications Cloud Native Core, Binding Support Function User Guide*.
- **Support for TLS in Diameter Gateway**: BSF uses Diameter Gateway to establish secured connections with consumer NFs and producer NFs, respectively. These communication protocols are encrypted using Transport Layer Security (TLS). For more information, see *"Support for TLS Using Diameter Gateway"* section in *Oracle Communications Cloud Native Core, Binding Support Function User Guide*.
- **BSF Message Feed for Monitoring**: In order to enable correlation of the internal and external (request/response) messages for all the transactions initiated by the producer and consumer NFs, BSF allows to copy the messages at Ingress and Egress Gateways. The analysis of these messages enable NFs to integrate with external 5G SBI monitoring system for call tracing/tracking and live debugging. For more information, see *"BSF Message Feed for Monitoring"* section in *Oracle Communications Cloud Native Core, Binding Support Function User Guide*.

2.3 Cloud Native Environment (CNE)

Release 24.3.3

Oracle Communications Cloud Native Core, Cloud Native Environment (CNE) 24.3.3 has been updated with the following enhancement:

CNLB: Multus Thick Plugin: In this release, *Multus thin plugin* is replaced with *Multus thick plugin*. As part of this change, for all new CNE installations with CNLB-enabled option, Multus thick plugin also gets installed. It is highly recommended to use Multus thick plugin based release for CNLB-based CNE deployments.

CNE release 24.3.3 and above support Multus Thick Plugin.

Release 24.3.2

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

Release 24.3.1

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

> ⓘ **Note**
>
> This is a maintenance release to incorporate code changes to support seamless upgrade from this release. These code changes do not have any impact on the performance or functioning of CNE.

Release 24.3.0

Oracle Communications Cloud Native Core, Cloud Native Environment (CNE) 24.3.0 includes the following enhancements:

- **Traffic Segregation: Cloud Native Load Balancer (CNLB) Support for BareMetal:** In the previous release, CNE provided Cloud Native Load Balancer (CNLB) for managing networks used for ingress and egress traffic, as an alternate to the existing LBVM, lb-controller, and egress-controller solution. This feature was supported for vCNE deployments (OpenStack and VMware). In this release, CNE extends CNLB support for BareMetal deployments. CNLB supports two ways to achieve network segregation in BareMetal deployments:
  - Using bond0 on hosts
  - Using VLANs on hosts

  CNE continues to support MetalLB and ToR based network segregation in BareMetal deployments. You can enable or disable this feature only at the time of a fresh CNE installation. For more information about enabling and configuring this feature for BareMetal, see *Oracle Communications Cloud Native Core, Cloud Native Environment User Guide* and *Oracle Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide*.
- **Floating IP Support for OpenStack API**: Floating IPs are additional public IP addresses that are associated to instances such as control nodes, worker nodes, Bastion Host, and LBVMs. Floating IPs can be quickly re-assigned and switched from one instance to another using API, thereby ensuring high availability and less maintenance. In the previous releases, CNE supported only fixed IP addresses for OpenStack deployments. With this

feature, CNE provides an option to associate floating IP addresses to all control nodes, worker nodes, Bastion Host, and LBVMs. For more information about this feature, see the *"Enabling or Disabling Floating IP"* section *Oracle Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide*.

- **Support for TLS**: With this feature, CNE extends its support for Transfer Layer Security (TLS) 1.3. In this release, the minimum supported TLS version for CNE internal and external communication is TLS 1.2. This means that CNE 24.3.0 will support both TLS 1.2 and TLS 1.3. However, in the upcoming releases, CNE will end its support for TLS 1.2 and support only TLS 1.3 for security and governance compliance.
- **New Versions of Common Services**: The following common services are upgraded in this release:
  - Helm - 3.15.2
  - Kubernetes - 1.30.0
  - containerd - 1.7.16
  - Calico - 3.27.3
  - Prometheus - 2.52.0
  - HAProxy - 3.0.2
  - Jaeger - 1.60.0
  - Istio - 1.18.2
  - Kyverno - 1.12.5
  - Prometheus Operator: 0.76.0

  To get the complete list of third-party services and their versions, refer to the dependencies_24.3.0.tgz file provided as part of the software delivery package.

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

- **GRUB Password Customization**: CNE provides the capability to customize the GRUB password to perform maintenance tasks on the boot in every host or member of the cluster. Depending on the type of cluster, you must add or modify the occne_grub_passwordvariable in the hosts.ini or occne.ini file during an installation or upgrade. This variable is mandatory for installation and upgrade. When you customize the GRUB password, ensure that the GRUB password meets the following conditions:
  - Contains at least eight characters.
  - Contains uppercase and lowercase characters.
  - Contains at least one special character: \, %, &, and $. The password can be enclosed with single or double quotes (" or '), however quotes cannot be a part of the password.
  - Contains at least two digits.

  For more information about this functionality, see *Oracle Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide*.
- **Container Security Enhancement**: In this release, CNE has improved the container security by enhancing securityContext values, adding new policy controls through Kyverno, and removing exec access to containers. A new Kyverno policy, require-emptydir-requests-and-

limits, is added in audit mode to provide insight about policy violations in pods. This policy will be enforced in the up coming releases. For more information about Kyverno policy management, the *"Managing Kyverno"* section in *Oracle Communications Cloud Native Core, Cloud Native Environment User Guide.*

Operations Services Overlay

Release 24.3.1

Oracle Communications Operations Services Overlay 24.3.1 has been updated with the following enhancement:

Support for new versions: 24_3_common_pod is replaced with 24_3_common_oso. For more information, see *Oracle Communications Operations Services Overlay Installation and Upgrade Guide*.

Release 24.3.0

Oracle Communications Operations Services Overlay 24.3.0 has been updated with the following enhancement:

Support for new versions:

24_2_common_pod is replaced with 24_3_common_pod.

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

2.4 Cloud Native Core cnDBTier

Release 24.3.1

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

Release 24.3.0

Oracle Communications Cloud Native Core, cnDBTier (cnDBTier) 24.3.0 includes the following enhancements:

- **Transparent Data Encryption (TDE)**: cnDBTier uses Transparent Data Encryption (TDE) to encrypt the data at the storage layer (the files stored in the disk or PVC of data nodes). TDE encrypts and decrypts data dynamically as it is written to or read from the storage, without requiring any modifications to the application's code. This guarantees that the sensitive data stored in the database files on disk remains encrypted while at rest, offering a crucial security layer against unauthorized access, particularly in situations where physical security controls fail. For more information, see *Oracle Communications Cloud Native Core, cnDBTier User Guide* and *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*.
- **Enhancement to Georeplication Recovery**: With this enhancement, cnDBTier has improved the rate at which the backup files are transferred between sites during a georeplication recovery. This improvement is achieved by:
  - using Secure File Transfer Protocol (SFTP) instead of CURL to transfer backup files between sites.
  - configuring a separate parameter (numberofparallelbackuptransfer) to perform the parallel transfer of backups in the data nodes. For more information about this parameter, see the *"Customizing cnDBTier"* section in *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*.

- **Oracle Cloud Infrastructure (OCI) Enablement**: In this release, cnDBTier has validated the proper functioning of the following procedures on OCI:
  - TLS support for georeplication.
  - Horizontal and vertical scaling of cnDBTier pods.
    For more information about these procedures, see *Oracle Communications Cloud Native Core, cnDBTier User Guide*.
- **Support for New Versions of Software**: Oracle MySQL Cluster Database version has been updated to 8.4.2.

> **Note**
>
> The following APIs are used to fetch cnDBTier status in a cached mode. This means that, the data returned by these APIs are from cached memory and are not dynamic. In previous releases, cnDBTier provided APIs which can fetch real-time status of cnDBTier clusters and replace the cached APIs. Therefore, cnDBTier plans to deprecate these APIs in a future release.

Cached API	Purpose	Replacement API
http://<base-uri>/db-tier/status/local	To fetch local cluster status	http://<base-uri>/ocdbtier/status/cluster/local/realtime
http://<base-uri>/db-tier/status/replication/{mate-site-name}	To fetch site-specific replication status	http://<base-uri>/ocdbtier/status/replication/realtime/{remoteSiteName}
http://<base-uri>/db-tier/status/replication	To fetch overall replication status	http://<base-uri>/ocdbtier/status/replication/realtime

2.5 Cloud Native Configuration Console (CNC Console)

Release 24.3.0

Oracle Communications Cloud Native Configuration Console (CNC Console) 24.3.0 includes the following enhancements:

- **Support for TLS with Automated Certificate Management**: CNC Console supports automation of certificate lifecycle management in integration with Oracle Communications Cloud Native Core, Certificate Manager (OCCM). This allows you to automatically create, renew, and delete certificates for a given CA, with the possibility to track previously created certificates and renew or delete them when required. For more information about OCCM, see the *"Support for Automated Certificate Lifecycle Management"* section in *Oracle Communications Cloud Native Configuration Console User Guide*, *Oracle Communications Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide*, and *Oracle Communications Cloud Native Core, Certificate Management User Guide*.
- **Support for Traffic Segregation**: CNC Console supports network segregation using Cloud Native Load Balancer (CNLB) to effectively manage ingress and egress traffic flows. CNE provides Cloud Native Load Balancer (CNLB) for managing networks used for ingress and egress traffic, as an alternate to the existing LBVM, lb-controller, and egress-controller solution. When this feature is enabled, CNE automatically uses CNLB to control ingress traffic. For managing the egress traffic, you must preconfigure the egress network details in the cnlb.ini file before installing CNE. This feature implements a least connection algorithm for IP Virtual Server (IPVS) based ingress distribution. For more information, see

Oracle Communications Cloud Native Configuration Console User Guide and *Oracle Communications Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide*.

- **Support for Dual Stack (IPv6 preferred) on Dual Stack IPv4 preferred Infrastructure**: CNC Console can be deployed with IPv4 or IPv6 or both simultaneously. For more information, see *Oracle Communications Cloud Native Configuration Console User Guide* and *Oracle Communications Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide*.
- **Support the Latest Version of NFs**: CNC Console provides support for the following NFs, OCCM, and Data Director:
  - SCP 24.3.x
  - NRF 24.3.x
  - UDR 24.3.x
  - Policy 24.3.x
  - BSF 24.3.x
  - OCCM 24.3.x
  - SEPP 24.3.x
  - NSSF 24.3.x
  - NEF 24.2.x
  - CAPIF 24.3.x
  - Data Director 24.3.x
  - NWDAF 24.3.x

  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*.

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

Release 24.3.0

Oracle Communications Cloud Native Core, Certificate Management (OCCM) 24.3.0 includes the following enhancements:

- **Improvements to Certificate Monitoring:** The monitoring certificates functionality enables you to monitor and manage previously created certificates. It enables you to identify and take action if certificates are modified or deleted manually, without experiencing loss of service. Certificate monitoring is performed in the following scenarios:
  - The certificate or the Kubernetes secret holding the certificate is deleted. An alert is raised and recreation of the certificate is triggered.
  - If the certificate is manually updated, then OCCM detects the change in the certificate and resets the monitoring. OCCM also validates if the manually filled certificate meets the certificate parameters, that is, Subject, Extended Key Usage, and so on. If the certificate does not match the requirements, an alert is raised. For more information, see *Oracle Communications Cloud Native Core, Certificate Management User Guide*.

- **Support for Traffic Segregation:** OCCM supports traffic segregation to specifically manage and control egress traffic, meaning all outgoing data and communication from OCCM to Certificate Authorities (CAs). This ensures that the traffic directed towards CAs is properly segregated and managed to maintain security and efficiency. In contrast, any incoming traffic, that is, REST API requests, is handled separately via the CNC Console. The CNC Console is responsible for managing and processing these incoming requests, ensuring that they are appropriately routed and secured. For information about enabling traffic segregation for OCCM deployment, see *Oracle Communications Cloud Native Core, Certificate Management Installation, Upgrade, and Fault Recovery Guide*.
- **Support for Certificate and Certificate Chain in the Same Kubernetes Secret or Key:** OCCM certificate configuration is enhanced to provide an option to fill certificate and certificate chain into a single file. For more information, see *Oracle Communications Cloud Native Core, Certificate Management User Guide*.

2.7 OCI Adaptor

Release 24.3.0

Oracle Communications Cloud Native Core, OCI Adaptor 24.3.0 includes the following enhancements:

- **Uplifted the OCI Adaptor Components**: The following OCI Adaptor components have been uplifted:
  - Management-agent is uplifted from 1.3.0 to 1.5.0.
  - Fluentd is uplifted from 1.4.1 to 1.5.0.
  - Metric-Server is uplifted from 0.6.4 to v0.7.2.
  - OTEL Collector is uplifted from 0.84.0 to 0.108.0.

2.8 Policy

Release 24.3.0

Oracle Communications Cloud Native Core, Converged Policy 24.3.0 includes the following enhancements:

- **Enhancements to Pending transaction Gx**: Policy has been enhanced to support configuration change for response timeout. The diameter configuration response timeout must be configured till the retry exhausts. The response timeout must be updated in the CNC Console. For more information, see *"Pending Transactions on Gx Interface"* section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.
- **Logging Support for Error Response in Policy**: Policy sends error responses to consumer NFs due to some exceptions, such as signaling, validations, and internal errors. These error responses have payloads containing the problem title, status, details, and cause of the error that are used to investigate the error. This feature enhances the logging mechanism to support detailed and enhanced logging. For more information, see *"Logging Support for Error Response in Policy"* section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.
- **Support for TLS**: Policy supports TLS 1.3 for all functions and interfaces that are supported by TLS 1.2. With this feature, Policy supports the creation of TLS 1.3 and TLS 1.2 connections and mandatory ciphers and extensions. These communication protocols are encrypted using Transport Layer Security (TLS). For more information, see "Support

for TLS" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.

- **PCRF Core Pod Congestion Control**: The PCRF Core service supports Pod Congestion Control mechanism that helps to handle heavy traffic of incoming requests. It considers every incoming request and decides to either reject or accept it based on a defined request priority and the status of service congestion level. For more information, see *"PCRF Core Pod Congestion Control"* section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.
- **UE Service Pod Congestion Control**: The UE service supports Pod Congestion Control mechanism that helps to handle heavy traffic of incoming requests. It considers every incoming request and decides to either reject or accept it based on a defined request priority and the status of service congestion level. For more information, see *"UE Service Pod Congestion Control"* section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.
- **Support for Diameter Message Response Time Latency Metrics**: The support for timer latency metrics in Diameter Gateway service provides the time taken to service a request/ response in Diameter call flows. This ensures that the cnPolicy meets the required service level agreements (SLAs) for latency by the customer. For more information, see *"Support for Diameter Message Response Time Latency Metrics"* section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.
- **PDS Performance Improvement**: The PDS service supports primary key based searches in its database. With this PDS service search, speed and performance are significantly improved, thereby streamlining operations and improving user experience. For more information, see *"PDS Settings"* section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.
- **Support for cnDBTier APIs in CNC Console**: The Policy CNC Console GUI supports integration of read-only Georeplicaiton Recovery (GRR) cnDBTier APIs. This functionality allows users to have specific information on cnDBTier statuses on the CNC Console. For more information, see *"Support for cnDBTier APIs in CNC Console"* section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.
- **Traffic Segregation**: Policy supports end-to-end traffic segregation based on traffic types. This ensures that critical networks are not cross-connected or share the same routes, thereby preventing network congestion. For more information, see *"Traffic Segregation"* section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.
- **Stale request cleanup for PCRF-Core service**: A request is considered as stale if the time taken for a request to be received by PCRF Core is more than the maximum timeframe mentioned in the request header. Similarly, if the time taken by the PCRF Core to process the received request and send its response back to the requestor such as Diameter Gateway or Ingress Gateway is more than the timeframe specified, such a response is considered as stale response. PCRF Core stops further processing of such stale requests and responses and sends a 13002 (DIAMETER_ERROR_TIMED_OUT_REQUEST) error to Diameter Gateway. For more information, see *"Support for Stale Requests Cleanup"* section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.
- **Stale request cleanup for SM service**: A request is considered as stale if the time taken for a request to be received by the SM service is more than the maximum timeframe mentioned in the request header. Similarly, if the time taken by SM service to process the received request and send its response back to the requestor such as Diameter Gateway or Ingress Gateway is more than the timeframe specified, such a response is considered as stale response. SM service stops further processing of such stale requests and responses and sends a 504 error to the requested NF. For more information, see *"Support*

for Stale Requests Cleanup" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.

- **Signaling and DB access processing latency histogram metrics for PCRF-Core service**: New histogram metrics on signaling and DB access processing latency are added to PCRF Core metrics. These new histogram metrics allow the monitoring of latency on PCRF Corecall flows such as response to diameter requests, HTTP incoming and outgoing connections, and DB requests. For more information, see *"PCRF Core Metrics"* section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.
- **Signaling and DB access processing latency histogram metrics for PDS service**: New histogram metrics on signaling and DB access processing latency are added to PolicyDS metrics. These new metrics allow to monitor latency distribution for the HTTP services inside PCF. Also, these metrics helps to get a variety of information, which enable to easily track the different transactions through PDS and measuring their performance. This is helpful in debugging and tracking of the PDS flows. For more information, see *"PolicyDS Metrics"* section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.
- **Support for End-to-End Log Identifier across Policy Services**: This feature allows to use a unique identifier to every log message, which can be used to identify the set of logs belonging to a given session across all Policy services. For more information, see *"Support for Unique Log Identifier Across Policy Services"* section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.

2.9 Network Repository Function (NRF)

Release 24.3.0

Oracle Communications Cloud Native Core, Network Repository Functions (NRF) 24.3.0 includes the following enhancements:

- **Support for Georeplication Recovery APIs in CNC Console**: With this enhancement, NRF can mark the disrupted cnDBTier cluster as failed, initiate georeplication recovery, and continuously monitor their status, ensuring seamless disaster recovery operations using CNC Console. For more information, see *"Support for cnDBTier APIs in CNC Console"* in *Oracle Communications Cloud Native Core, Network Repository Function User Guide*.
- **Upgrade and Rollback Enhancement:** NRF now supports N-2 releases upgrade and rollback, where N indicates the current release version of NRF. For NRF release 24.3.0, the upgrade paths can be from 24.1.x or 24.2.x. Similarly, for NRF release 24.3.0, the rollback paths can be 24.2.x or 24.1.x. For more information about this enhancement, see *“Supported Upgrade Paths”* and *“Supported Rollback Paths”* in *Oracle Communications Cloud Native Core, Network Repository Function Installation, Upgrade, and Fault Recovery Guide*.
- **Enhancements for dnn NFProfile Attribute and Discovery Query Parameter**: As per 3GPP TS 29.571 v16.7, from 24.3.x release, NRF supports additional validations for the dnn attribute during NFManagement and NFDiscover service operations. NRF also supports exact or partial matching of dnn query attribute value with the dnn attribute present in the registered NFProfile for NFDiscover service operation. For more information, see *"NRF Compliance Matrix and Enhancements for dnn NFProfile Attribute and Discovery Query Parameter"* section in *Oracle Communications Cloud Native Core, Network Repository Function User Guide*.
- **Support for servingClientTypes in LMFInfo and GMLCInfo**: As per 3GPP TS 29.510 v16.7, NRF supports servingClientTypes attribute in NF Profiles for Location Management Function (LMC) (LmfInfo) and Gateway Mobile Location Center (GMLC) (GmlcInfo). NRF

supports client-type discovery query parameter to discover NFs based on servingClientTypes. If the above mentioned attributes are present in the NF Profile, then the GMLC and LMF NFs are considered as dedicated to serve the listed external client type. The listed external client types are mentioned in 3GPP TS 29.572 v16.7. If this attribute is not present in the NF Profile for the mentioned NFTypes, then NFs are not considered as dedicated to serve any external client type. For more information, see *"NRF Compliance Matrix and Support for servingClientTypes in LMFInfo and GMLCInfo"* section in *Oracle Communications Cloud Native Core, Network Repository Function User Guide*.

- **Support for Server Header:** NRF handles various requests from Consumer Network Functions (NFs) and other network entities over HTTP protocol. Upon receiving these requests, NRF validates and processes these requests before responding to Consumer NFs. If NRF sends an error response, then the consumer NFs need to know the source of the error for troubleshooting and to take corrective measures. This feature adds server headers to the error response generated by NRF, which is useful in identifying the origin of an error. This enhancement improves NRF’s error handling for better troubleshooting and corrective actions by the consumer NFs. For more information, see the *"Support for Server Header"* section in *Oracle Communications Cloud Native Core, Network Repository Function User Guide*.

2.10 Network Slice Selection Function (NSSF)

Release 24.3.2

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

Release 24.3.1

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

Release 24.3.0

Oracle Communications Cloud Native Core, Network Slice Selection Function (NSSF) 24.3.0 includes the following enhancements:

- **Support for TLS in NSSF**: In addition to TLS 1.2, NSSF now supports TLS 1.3 encryption to establish secure HTTPS connections. TLS 1.3 simplifies the handshake process by reducing round trips and enhancing security with improved encryption, compared to TLS 1.2. This version also supports Perfect Forward Secrecy (PFS), which secures session keys independently of long-term private keys and uses stronger cipher suites for improved privacy. While TLS 1.3 is prioritized, TLS 1.2 remains supported to ensure compatibility. For more information, see the *"Support for TLS in NSSF"* section in the *Oracle Communications Cloud Native Core, Network Slice Selection Function User Guide*.
- **Traffic Segregation**: This feature provides end-to-end traffic segregation to NSSF based on traffic types. It addresses the challenge of logically separating IP traffic of different profiles, which are typically handled through a single network (Kubernetes overlay). The Multus CNI container network interface (CNI) plugin for Kubernetes allows to attach multiple network interfaces to pods to help segregate traffic from each NSSF microservice. The new functionality ensures that critical networks are not cross-connected or sharing the same routes, thereby preventing network congestion. For more information, see the *"Traffic Segregation"* section in the *Oracle Communications Cloud Native Core, Network Slice Selection Function User Guide*.

2.11 Service Communication Proxy (SCP)

Release 24.3.0

Oracle Communications Cloud Native Core, Service Communication Proxy (SCP) 24.3.0 includes the following enhancements:

- **SCP Response Timeout Extension**: With this enhancement, SCP allows users to extend the maximum response timeout to 50 seconds. This improvement provides configuration options to support response timeouts for NFs that require more time to serve a request. For more information, see the *"SCP Response Timeout Extension"* section in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.
- **Verbose Logging for SCP**: This enhancement introduces verbose logging specifically for the SCPC-Audit microservice within the control plane. For more information, see the *"Verbose Logging for SCP"* section in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.
- **Log Enhancement for 5G SBI Error Responses Generated by SCP**: SCP has enhanced the error logs by including information, such as sender details, subscriber ID, error status code, error title, error details, and error cause. These details, along with the problem details, identify the cause of the error responses generated by SCP. For more information, see the *"Log Enhancement for 5G SBI Error Responses Generated by SCP"* section in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.

2.12 Security Edge Protection Proxy (SEPP)

Release 24.3.2

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

Release 24.3.1

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

Release 24.3.0

Oracle Communications Cloud Native Core, Security Edge Protection Proxy (SEPP) 24.3.0 includes the following enhancements:

- **Security Countermeasure Non-Verbose Error Responses:** With this enhancement, SEPP's security countermeasure features have been improved to provide either detailed (verbose) or concise (non-verbose) error responses, depending on user configurations. In this release, the error response configurations of the following features are enhanced:
  - Cat-0 SBI Message Schema Validation Feature
  - Cat-1 Service API Validation Feature
  - Cat-2 Network ID Validation Feature
  - Cat-3 Previous Location Check Feature

  When verbose error responses are disabled, attributes such as title, detail, and cause in the error response are filled with less detailed, user-configured values. By default, these attributes are set to "Rejected" for title, "Server Error" for detail, and "Unknown" for cause. Http status code remains same as earlier. Additionally, attributes like invalidParams and instances are not included in the generated error responses.When verbose error responses are enabled, all security countermeasure features display verbose (detailed) error responses, similar to those in previous SEPP releases.

For more information about the feature, see *"Security Countermeasure Non-verbose Error Responses"* section in *Oracle Communications Cloud Native Core, Security Edge Protection Proxy User Guide, Oracle Communications Cloud Native Core, Security Edge Protection Proxy REST API Guide,* and *Oracle Communications Cloud Native Core, Security Edge Protection Proxy Troubleshooting Guide.*

- **Multiple SEPP Instances on Shared cnDBTier Cluster:**
  Oracle Communications Cloud Native Core, Security Edge Protection Proxy (SEPP) now supports a new deployment model that allows multiple SEPP instances to be deployed on a shared cnDBTier cluster. This approach optimizes resource utilization, as SEPP is a stateless service, and the existing cnDBTier often operates below capacity.

  Using a shared cnDBTier for multiple SEPP instances can save a significant amount of CPU resources compared to having a separate database for each instance. This shared cnDBTier is built with security features that restrict data access for each SEPP instance by using unique logins and credentials during deployment. This allows each SEPP instance to securely access its own database while using the same cnDBTier within the Kubernetes cluster. For example, deploying four SEPP instances in the same cluster can lead to considerable increase resource efficiency compared to giving each instance its own database.

  In this deployment model, 1+1 GR redundancy only supported with maximum four SEPP instances in one cluster to avoid operational scaling issues. This deployment model can only be used for SEPP instances deployed on the same CNE cluster.

  For more information about the feature, see *"Multiple SEPP Instances on Shared cnDBTier Cluster"* section in *Oracle Communications Cloud Native Core, Security Edge Protection Proxy User Guide, Oracle Communications Cloud Native Core, Security Edge Protection Proxy REST API Guide,* and *Oracle Communications Cloud Native Core, Security Edge Protection Proxy Troubleshooting Guide.*

- **Proactive Status Updates on SEPP:** In the previous releases, consumer NFs sent Service Based Interface (SBI) message requests to SEPP without checking the status of SEPP because there was no health check mechanism implemented at SEPP.
  Using this feature, consumer NFs can determine the health or connection status of SEPP before forwarding any SBI message request to SEPP. This feature allows consumer NFs or consumer SEPPs to perform the following health check verification at SEPP:

  - Determines if SEPP is reachable through the transport path.
  - Determines if SEPP is available to respond to SBI message requests.

  For more information about the feature, see the *"Proactive Status Updates on SEPP"* section in *Oracle Communications Cloud Native Core, Security Edge Protection Proxy User Guide*, *Oracle Communications Cloud Native Core, Security Edge Protection Proxy REST API Guide,* and *Oracle Communications Cloud Native Core, Security Edge Protection Proxy Troubleshooting Guide.*

- **Traffic Segregation:** This feature provides end-to-end traffic segregation to SEPP based on traffic types. Within a Kubernetes cluster, traffic segregation can divide applications or workloads into distinct sections such as OAM, SBI, Kubernetes control traffic, and so on. The Multus CNI container network interface (CNI) plugin for Kubernetes allows to attach multiple network interfaces to pods to help segregate traffic from each SEPP microservice. This feature addresses the challenge of logically separating IP traffic of different profiles, which are typically handled through a single network (Kubernetes overlay). The new functionality ensures that critical networks are not cross-connected or sharing the same routes, thereby preventing network congestion. For more information about the feature, see the *"Traffic Segregation"* section in *Oracle Communications Cloud Native Core, Security Edge Protection Proxy User Guide.*

2.13 Unified Data Repository (UDR)

Release 24.3.0

Oracle Communications Cloud Native Core, Unified Data Repository (UDR) 24.3.0 includes the following enhancements:

- **IMSI Fallback Lookup Enhancement**: This feature enables Equipment Identity Register (EIR) to return user equipment status as WHITELISTED, BLACKLISTED, or GREYLISTED for the matched International Mobile Equipment Identity (IMEI) in the EIR database. For more information, see *"IMSI Fallback Lookup Enhancement"* section in *Oracle Communications Cloud Native Core, Unified Data Repository User Guide*.
- **Diameter S13 Interface:** This feature supports diameter interface between EIR and Mobility Management Entity (MME) to retrieve the User Equipment (UE) status of the subscriber from the EIR database. For more information, see *"Diameter S13 Interface"* section in *Oracle Communications Cloud Native Core, Unified Data Repository User Guide*.
- **Secure File Transfer Support for Subscriber Bulk Import Tool Enhancement**: This feature is enhanced to support separate file paths for PDBI files and result log files. For more information, see *"Secure File Transfer Support for Subscriber Bulk Import Tool Enhancement"* section in *Oracle Communications Cloud Native Core, Unified Data Repository User Guide*.

3
Media and Documentation

3.1 Media Pack

This section lists the media package for Oracle Communications Cloud Native Core 3.24.3. To download the media package, see MOS.

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

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

Table 3-1 Media Pack Contents for Oracle Communications Cloud Native Core 3.24.3

Description	NF Version	ATS Version	Upgrade Supported
Oracle Communications Cloud Native Core, Binding Support Function (BSF)	24.3.0	24.3.0	BSF 24.3.0 supports fresh installation and upgrade from 24.2.x and 24.1.x. For more information, see *Oracle Communications Cloud Native Core, Binding Support Function Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Configuration Console (CNC Console)	24.3.0	NA	CNC Console 24.3.0 supports fresh installation and upgrade from 24.2.x and 24.1.x. For more information, see *Oracle Communications Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide.* **Note**: CNC Console supports N-2 NF versions during upgrade window. For example, CNC Console 24.3.0 supports SCP 24.3.0, 24.2.x, and 24.1.x. Any newly added features in Console which have NF dependency in latest release may not be available in previous release.
Oracle Communications Cloud Native Core, cnDBTier (cnDBTier)	24.3.1	NA	cnDBTier 24.3.1 supports fresh installation and upgrade from 24.3.0, 24.2.x and 24.1.x. For more information, see *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*.

Table 3-1 (Cont.) Media Pack Contents for Oracle Communications Cloud Native Core 3.24.3

Description	NF Version	ATS Version	Upgrade Supported
Oracle Communications Cloud Native Core, cnDBTier (cnDBTier)	24.3.0	NA	cnDBTier 24.3.0 supports fresh installation and upgrade from 24.2.x and 24.1.x. For more information, see *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Cloud Native Environment (CNE)	24.3.3	NA	CNE 24.3.3 supports fresh installation and upgrade from 24.3.x and 24.2.x. For more information, see *Oracle Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide.*
Oracle Communications Cloud Native Core, Cloud Native Environment (CNE)	24.3.2	NA	CNE 24.3.2 supports fresh installation and upgrade from 24.3.x and 24.2.x. For more information, see *Oracle Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Cloud Native Environment (CNE)	24.3.1	NA	CNE 24.3.1 supports fresh installation and upgrade from 24.3.0 and 24.2.x. For more information, see *Oracle Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Cloud Native Environment (CNE)	24.3.0	NA	CNE 24.3.0 supports fresh installation and upgrade from 24.2.x. For more information, see *Oracle Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Certificate Management (OCCM)	24.3.0	NA	OCCM 24.3.0 supports fresh installation and upgrade from 24.1.x and 24.2.x. For more information, see *Oracle Communications Cloud Native Core, Certificate Management Installation, Upgrade, and Fault Recovery Guide.*
Oracle Communications Cloud Native Core, Network Repository Function (NRF)	24.3.0	24.3.0	NRF 24.3.0 supports fresh installation and upgrade from 24.1.x and 24.2.x. For more information, see *Oracle Communications Cloud Native Core, Network Repository Function Installation, Upgrade, and Fault Recovery Guide*.

Table 3-1 (Cont.) Media Pack Contents for Oracle Communications Cloud Native Core 3.24.3

Description	NF Version	ATS Version	Upgrade Supported
Oracle Communications Cloud Native Core, Network Slice Selection Function (NSSF)	24.3.2	24.3.2	NSSF 24.3.2 supports fresh installation and upgrade from 24.2.x and 24.3.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, Network Slice Selection Function (NSSF)	24.3.1	24.3.1	NSSF 24.3.1 supports fresh installation and upgrade from 24.3.0. For more information, see *Oracle Communications Cloud Native Core, Network Slice Selection Function Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Network Slice Selection Function (NSSF)	24.3.0	24.3.0	NSSF 24.3.0 supports fresh installation and upgrade from 24.2.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)	24.3.0	24.3.0	Policy 24.3.0 supports fresh installation and upgrade from 24.2.x and 24.1.x. For more information, see *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, OCI Adaptor	24.3.0	NA	OCI Adaptor supports fresh installation only. For more information, see *Oracle Communications Cloud Native Core, OCI Deployment Guide*.
Oracle Communications Operations Services Overlay (OSO)	24.3.1	NA	OSO 24.3.1 supports fresh installation. For more information, see *Oracle Communications Operations Services Overlay Installation and Upgrade Guide*.
Oracle Communications Operations Services Overlay (OSO)	24.3.0	NA	OSO 24.3.0 supports fresh installation. For more information, see *Oracle Communications Operations Services Overlay Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core, Service Communications Proxy (SCP)	24.3.0	24.3.0	SCP 24.3.0 supports fresh installation and upgrade from 24.2.x and 24.1.x. For more information, see *Oracle Communications Cloud Native Core, Service Communication Proxy Installation, Upgrade, and Fault Recovery Guide*.

Table 3-1 (Cont.) Media Pack Contents for Oracle Communications Cloud Native Core 3.24.3

Description	NF Version	ATS Version	Upgrade Supported
Oracle Communications Cloud Native Core, Security Edge Protection Proxy (SEPP)	24.3.2	24.3.0	SEPP 24.3.2 supports fresh installation and upgrade from 24.3.x, 24.1.x, and 24.2.x. For more information, see *Oracle Communications Cloud Native Core, Security Edge Protection Proxy Installation, Upgrade, and Fault Recovery Guide.*
Oracle Communications Cloud Native Core, Security Edge Protection Proxy (SEPP)	24.3.1	24.3.0	SEPP 24.3.1 supports fresh installation and upgrade from 24.3.0, 24.1.x, 24.2.0, 24.2.1, and 24.2.3. Upgrade from 24.2.4 is not supported to this release. For more information, see *Oracle Communications Cloud Native Core, Security Edge Protection Proxy Installation, Upgrade, and Fault Recovery Guide.*
Oracle Communications Cloud Native Core, Security Edge Protection Proxy (SEPP)	24.3.0	24.3.0	SEPP 24.3.1 supports fresh installation and upgrade from 24.3.0, 24.1.x, 24.2.0, 24.2.1, and 24.2.3. Upgrade from 24.2.4 is not supported to this release. 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)	24.3.0	24.3.0	UDR 24.3.0 supports fresh installation and upgrade from 24.1.x and 24.2.x. For more information, see *Oracle Communications Cloud Native Core, Unified Data Repository Installation, Upgrade, and Fault Recovery Guide*.

3.2 Compatibility Matrix

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

ⓘ **Note**

- For seamless integration and optimal performance of CNC NFs on third party platform, the third party platform needs to be compatible with the specified Kubernetes version.

Table 3-2 Compatibility Matrix

CNC NF	NF Version	CNE	cnDBTier	OSO	ASM S/W	Kubernetes	CNC Console	OCNADD	OCCM	OCI Adaptor
BSF	24.3.0	• 24.3.x • 24.2.x • 24.1.x	• 24.3.x • 24.2.x • 24.1.x	• 24.3.x • 24.2.x • 24.1.x	1.14.6	• 1.30.x • 1.29.x • 1.28.x	24.3.x	NA	24.3.x	NA
CNC Console	24.3.0	• 24.3.x • 24.2.x • 24.1.x	• 24.3.x • 24.2.x • 24.1.x	• 24.3.x • 24.2.x • 24.1.x	• 1.14.6 • 1.11.8 • 1.9.8	• 1.30.x • 1.29.x • 1.28.x	NA	24.3.x	24.3.x	24.3.x
cnDBTier	24.3.1	• 24.3.x • 24.2.x • 24.1.x	NA	NA	NA	• 1.30.x • 1.29.x • 1.28.x	NA	NA	NA	NA
cnDBTier	24.3.0	• 24.3.x • 24.2.x • 24.1.x	NA	NA	NA	• 1.30.x • 1.29.x • 1.28.x	NA	NA	NA	NA
CNE	24.3.3	NA	NA	NA	NA	1.30.x	NA	NA	NA	NA
CNE	24.3.2	NA	NA	NA	NA	1.30.x	NA	NA	NA	NA
CNE	24.3.1	NA	NA	NA	NA	1.30.x	NA	NA	NA	NA
CNE	24.3.0	NA	NA	NA	NA	1.30.x	NA	NA	NA	NA
NRF	24.3.0	• 24.3.x • 24.2.x • 24.1.x	• 24.3.x • 24.2.x • 24.1.x	• 24.3.x • 24.2.x • 24.1.x	1.14.6	• 1.30.x • 1.29.x • 1.28.x	24.3.x	24.3.x	24.3.x	24.3.x

Table 3-2 (Cont.) Compatibility Matrix

CNC NF	NF Version	CNE	cnDBTier	OSO	ASM S/W	Kubernetes	CNC Console	OCNADD	OCCM	OCI Adaptor
NSSF	24.3.2	• 24.3.x • 24.2.x • 24.1.x	• 24.3.x • 24.2.x • 24.1.x	• 24.3.x • 24.2.x • 24.1.x	1.1.4.6	• 1.30.x • 1.29.x • 1.28.x	24.3.x	NA	NA	NA
NSSF	24.3.1	• 24.3.x • 24.2.x • 24.1.x	• 24.3.x • 24.2.x • 24.1.x	• 24.3.x • 24.2.x • 24.1.x	1.1.4.6	• 1.30.x • 1.29.x • 1.28.x	24.3.x	NA	NA	NA
NSSF	24.3.0	• 24.3.x • 24.2.x • 24.1.x	• 24.3.x • 24.2.x • 24.1.x	• 24.3.x • 24.2.x • 24.1.x	1.1.4.6	• 1.30.x • 1.29.x • 1.28.x	24.3.x	NA	NA	NA
Policy	24.3.0	• 24.3.x • 24.2.x • 24.1.x	• 24.3.x • 24.2.x • 24.1.x	• 24.3.x • 24.2.x • 24.1.x	1.1.4.6	• 1.30.x • 1.29.x • 1.28.x	24.3.x	NA	24.3.x	NA
OCCM	24.3.0	• 24.3.x • 24.2.x • 24.1.x	NA	NA	NA	• 1.30.x • 1.29.x • 1.28.x	23.4.x	NA	NA	NA
OCI Adaptor	24.3.0	NA	• 24.3.x • 24.2.x • 24.1.x	NA	NA	• 1.30.x • 1.29.x • 1.28.x	24.3.x	NA	NA	NA

Table 3-2 (Cont.) Compatibility Matrix

CNC NF	NF Version	CNE	cnDBTier	OSO	ASM S/W	Kubernetes	CNC Console	OCNADD	OCCM	OCI Adaptor
OSO	24.3.1	NA	NA	NA	NA	• 1.30.x • 1.29.x • 1.28.x	NA	NA	NA	NA
OSO	24.3.0	NA	NA	NA	NA	• 1.30.x • 1.29.x • 1.28.x	NA	NA	NA	NA
SCP	24.3.0	• 24.3.x • 24.2.x • 24.1.x	• 24.3.x • 24.2.x • 24.1.x	• 24.3.x • 24.2.x • 24.1.x	• 1.14.6 • 1.11.8	• 1.30.x • 1.29.x • 1.28.x	24.3.x	24.3.x	24.3.x	24.3.x
SEPP	24.3.2	• 24.3.x • 24.2.x • 24.1.x	• 24.3.x • 24.2.x • 24.1.x	• 24.3.x • 24.2.x • 24.1.x	1.14.6	• 1.30.x • 1.29.x • 1.28.x	24.3.x	NA	24.3.x	24.3.x
SEPP	24.3.1	• 24.3.x • 24.2.x • 24.1.x	• 24.3.x • 24.2.x • 24.1.x	• 24.3.x • 24.2.x • 24.1.x	1.14.6	• 1.30.x • 1.29.x • 1.28.x	24.3.x	NA	24.3.x	24.3.x
SEPP	24.3.0	• 24.3.x • 24.2.x • 24.1.x	• 24.3.x • 24.2.x • 24.1.x	• 24.3.x • 24.2.x • 24.1.x	1.14.6	• 1.30.x • 1.29.x • 1.28.x	24.3.x	NA	24.3.x	24.3.x

Table 3-2 (Cont.) Compatibility Matrix

CNC NF	NF Version	CNE	cnDBTier	OSO	ASM S/W	Kubernetes	CNC Console	OCNADD	OCCM	OCI Adaptor
UDR	24.3.0	- 24.3.x - 24.2.x - 24.1.x	- 24.3.x - 24.2.x - 24.1.x	- 24.3.x - 24.2.x - 24.1.x	- 1.1.4.6 - 1.11.8	- 1.30.x - 1.29.x - 1.28.x	24.3.x	NA	24.3.x	NA

3.3 3GPP Compatibility Matrix

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

Table 3-3 3GPP Compatibility Matrix

CNC NF	NF Version	3GPP
BSF	24.3.0	- 3GPP TS 23.501 v18.4.0 - 3GPP TS 23.502 v18.4.0 - 3GPP TS 23.503 v18.4.0 - 3GPP TS 29.500 v18.3.0 - 3GPP TS 29.510 v18.4.0 - 3GPP TS 29.510 v17.7.0 - 3GPP TS 29.513 V18.4.0 - 3GPP TS 29.521 v18.3.0 - 3GPP TS 33.501 v18.3.0
CNC Console	24.3.0	NA
cnDBTier	24.3.0	NA
CNE	24.3.x	NA
NRF	24.3.0	- 3GPP TS 29.510 v15.5 - 3GPP TS 29.510 v16.3.0 - 3GPP TS 29.510 v16.7 - 3GPP TS 29.510 v17.7
NSSF	24.3.x	- 3GPP TS 29.531 v15.5.0 - 3GPP TS 29.531 v16.5.0 - 3GPP TS 29.531 v16.8.0 - 3GPP TS 29.501 v16.10.0 - 3GPP TS 29.502 v16.10.0
NSSF	24.3.0	- 3GPP TS 29.531 v15.5.0 - 3GPP TS 29.531 v16.5.0 - 3GPP TS 29.531 v16.8.0 - 3GPP TS 29.501 v16.10.0 - 3GPP TS 29.502 v16.10.0
OCCM	24.3.0	- 3GPP TS 33.310-h30 - 3GPP TR 33.876 v.0.3.0
OSO	24.3.x	NA

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

CNC NF	NF Version	3GPP
Policy	24.3.0	• 3GPP TS 33.501 v17.7.0 • 3GPP TS 29.500 v17.12.0 • 3GPP TS 23.501 v17.10.0 • 3GPP TS 23.502 v17.10.0 • 3GPP TS 23.503 v17.10.0 • 3GPP TS 29.504 v17.12.0 • 3GPP TS 29.507 v17.10.0 • 3GPP TS 29.510 v17.11.0 • 3GPP TS 29.512 v17.12.0 • 3GPP TS 29.513 V17.12.0 • 3GPP TS 29.514 v17.9.0 • 3GPP TS 29.214 v17.4.0 • 3GPP TS 29.518 v17.12.0 • 3GPP TS 29.519 v17.12.0 • 3GPP TS 29.520 v17.11.0 • 3GPP TS 29.521 v17.9.0 • 3GPP TS 29.525 v17.9.0 • 3GPP TS 29.594 v17.5.0 • 3GPP TS 29.519 v15.5.0 • 3GPP TS 23.203 v16.2.0 • 3GPP TS 29.212 V16.3.0 • 3GPP TS 29.213 v16.3 • 3GPP TS 29.214 v16.2.0 • 3GPP TS 29.219 v16.0.0 • 3GPP TS 29.335 v16.0
SCP	24.3.0	• 3GPP TS 29.500 R16 v16.6.0 • 3GPP TS 29.501 R16 v16.5.0
SEPP	24.3.x	• 3GPP TS 23.501 v17.6.0 • 3GPP TS 23.502 v17.6.0 • 3GPP TS 29.500 v17.8.0 • 3GPP TS 29.501 v17.7.0 • 3GPP TS 29.573 v17.6.0 • 3GPP TS 29.510 v17.7.0 • 3GPP TS 33.501 v17.7.0 • 3GPP TS 33.117 v17.1.0 • 3GPP TS 33.210 v17.1.0
UDR	24.3.0	• 3GPP TS 29.505 v15.4.0 • 3GPP TS 29.504 v16.2.0 • 3GPP TS 29.519 v16.2.0 • 3GPP TS 29.511 v17.2.0

Note

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

3.4 Common Microservices Load Lineup

This section provides information about common microservices and ATS for the specific NF versions in Oracle Communications Cloud Native Core Release 3.24.3.

Table 3-4 Common Microservices Load Lineup for Network Functions

CNC NF	NF Version	Alternate Route Svc	App-Info	ASM Configuration	ATS Framework	Config-Server	Debug-tool	Egress Gateway	Ingress Gateway	Helm Test	Mediation	NRF-Client	Perf-Info
BSF	24.3.0	24.3.3	24.3.4	24.3.0	24.3.1	24.3.4	24.3.1	24.3.3	24.3.3	24.3.2	NA	24.3.2	24.3.4
CNC Console	24.3.0	NA	NA	NA	NA	NA	24.3.1	NA	24.3.3	24.3.2	NA	NA	NA
OCCM	24.3.0	NA	NA	NA	NA	NA	24.3.1	NA	NA	24.3.2	NA	NA	NA
NRF	24.3.0	24.3.3	24.3.3	24.3.0	24.3.1	NA	24.3.1	24.3.3	24.3.3	24.3.2	NA	NA	24.3.3
NSSF	24.3.2	24.3.6	24.3.3	24.3.2	24.3.1	24.3.3	24.3.1	24.3.6	24.3.6	24.3.2	NA	24.3.1	24.3.3
NSSF	24.3.1	24.3.3	24.3.3	24.3.1	24.3.1	24.3.3	24.3.1	24.3.3	24.3.3	24.3.2	NA	24.3.1	24.3.3
NSSF	24.3.0	24.3.3	24.3.3	24.3.0	24.3.1	24.3.3	24.3.1	24.3.3	24.3.3	24.3.2	NA	24.3.1	24.3.3
Policy	24.3.0	24.3.3	24.3.5	24.3.0	24.3.1	24.3.5	24.3.1	24.3.3	24.3.3	24.3.2	NA	24.3.2	24.3.5
SCP	24.3.0	NA	NA	24.3.0	24.3.1	NA	24.3.1	NA	NA	24.3.2	24.3.1	NA	NA
SEPP	24.3.2	24.3.5	24.3.3	24.3.0	24.3.1	24.3.3	24.3.1	24.3.5	24.3.5	24.3.2	24.3.1	24.3.4	24.3.3
SEPP	24.3.1	24.3.2	24.3.3	24.3.0	24.3.1	24.3.3	24.3.1	24.3.2	24.3.2	24.3.2	24.3.1	24.3.1	24.3.3
SEPP	24.3.0	24.3.2	24.3.3	24.3.0	24.3.1	24.3.3	24.3.1	24.3.2	24.3.2	24.3.2	24.3.1	24.3.1	24.3.3
UDR	24.3.0	24.3.3	24.3.3	24.3.0	24.3.1	24.3.3	24.3.1	24.3.3	24.3.3	24.3.2	NA	24.3.2	24.3.3

3.5 Security Certification Declaration

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

3.5.1 BSF Security Certification Declaration

Release 24.3.0

Table 3-5 BSF Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	Nov 4, 2024	No unmitigated critical or high findings

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

Compliance Test Description	Test Completion Date	Summary
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	Oct 8, 2024	No unmitigated critical or high findings
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	Nov 4, 2024	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	Nov 7, 2024	No findings

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

3.5.2 CNC Console Security Certification Declaration

Release 24.3.0

Table 3-6 CNC Console Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	Oct 29, 2024	No unmitigated critical or high findings
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	Oct 25, 2024	No unmitigated critical or high findings

Table 3-6 (Cont.) CNC Console Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	Oct 28, 2024	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	Oct 24, 2024	No findings

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

3.5.3 OCCM Security Certification Declaration

Release 24.3.0

Table 3-7 OCCM Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	Oct 22, 2024	No unmitigated critical or high findings
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	Oct 22, 2024	No unmitigated critical or high findings
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	Oct 23, 2024	No unmitigated critical or high finding

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

Compliance Test Description	Test Completion Date	Summary
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	Oct 23, 2024	No findings

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

3.5.4 NRF Security Certification Declaration

Release 24.3.0

Table 3-8 NRF Security Certification Declaration

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

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

3.5.5 NSSF Security Certification Declaration

Release 24.3.2

Table 3-9 NSSF Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	July 18, 2025	No unmitigated critical or high findings
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	July 18, 2025	No unmitigated critical or high findings
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	July 18, 2025	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	July 18, 2025	No findings

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

Release 24.3.1

Table 3-10 NSSF Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	Sep 11, 2024	No unmitigated critical or high findings

Table 3-10 (Cont.) NSSF Security Certification Declaration

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

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

Release 24.3.0

Table 3-11 NSSF Security Certification Declaration

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

Table 3-11 (Cont.) NSSF Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	Sep 11, 2024	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	Sep 11, 2024	No findings

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

3.5.6 Policy Security Certification Declaration

Policy 24.3.0

Table 3-12 Policy Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	Oct 31, 2024	No unmitigated critical or high findings
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	Oct 22, 2024	No unmitigated critical or high findings
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	Nov 04, 2024	No unmitigated critical or high finding

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

Compliance Test Description	Test Completion Date	Summary
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	Nov 15, 2024	No findings

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

3.5.7 SCP Security Certification Declaration

SCP 24.3.0

Table 3-13 SCP Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	Oct 2, 2024	No unmitigated critical or high findings
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	Oct 21, 2024	No unmitigated critical or high findings
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	Oct 21, 2024	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	Oct 21, 2024	No findings

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

3.5.8 SEPP Security Certification Declaration

Release 24.3.2

Table 3-14 SEPP Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	April 30, 2025	No unmitigated critical or high findings. Scan done through Fortify.
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	NA	No unmitigated critical, high, medium, and low findings. Scan done through RestFuzz.
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	NA	No unmitigated critical or high findings. Scan done through Blackduck.
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	April 30, 2025	No issues found. Scan done through McAfee.

Release 24.3.1

Table 3-15 SEPP Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	Feb 03, 2025	No unmitigated critical or high findings. Scan done through Fortify.

Table 3-15 (Cont.) SEPP Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	NA	No unmitigated critical, high, medium, and low findings. Scan done through RestFuzz.
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	NA	No unmitigated critical or high findings. Scan done through Blackduck.
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	Feb 04, 2025	No issues found. Scan done through McAfee.

Release 24.3.0

Table 3-16 SEPP Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	Oct 24, 2024	No unmitigated critical or high findings. Scan done through Fortify.
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	Sep 11, 2024	No unmitigated critical, high, medium, and low findings. Scan done through RestFuzz.
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	Oct 24, 2024	No unmitigated critical or high findings. Scan done through Blackduck.

Table 3-16 (Cont.) SEPP Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	Oct 25, 2024	No issues found. Scan done through McAfee.

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

3.5.9 UDR Security Certification Declaration

Release 24.3.0

Table 3-17 UDR Security Certification Declaration

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

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

3.6 Documentation Pack

All documents for Oracle Communications Cloud Native Core (CNC) 3.24.3 are available for download on SecureSites and MOS.

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

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

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

4

Resolved and Known Bugs

This chapter lists the resolved and known bugs for Oracle Communications Cloud Native Core release 3.24.3.

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

4.1 Severity Definitions

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

Severity 1

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

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

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

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

Severity 2

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

Severity 3

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

Severity 4

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

4.2 Resolved Bug List

The following Resolved Bugs tables list the bugs that are resolved in Oracle Communications Cloud Native Core Release 3.24.3.

4.2.1 BSF Resolved Bugs

Table 4-1 BSF 24.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36912417	BSF Management error handling feature is failing due to a missing validation when loading up new configurations	BSF Management error handling feature was failing due to a missing validation in new configurations.	3	24.2.0

ⓘ **Note**

Resolved bugs from 24.1.0 and 24.2.1 have been forward ported to Release 24.3.0.

4.2.2 CNC Console Resolved Bugs

Table 4-2 CNC Console 24.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36918008	High Memory usage observed with mcore-ingress-gateway pod and the logs showing "java.lang.OutOfMemoryError"	High memory usage was observed with the mcore-ingress-gateway pod, and the logs displayed "java.lang.OutOfMemoryError."	2	24.2.0
36784539	Unable to fetch the PCF user's session through REST API via CNCC.	It was not possible to fetch the PCF user's session through the REST API through CNC Console.	3	23.4.0
36950084	An issue in enabling IAM Keycloak logs	There was an issue with enabling IAM Keycloak logs. Log Level is changed to debug by default for event logging.	3	23.4.1

Table 4-2 (Cont.) CNC Console 24.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37102681	Changing settings for the IAM admin user via REST API	Changing settings for the IAM admin user through the REST API was not possible.	3	23.4.0
36672540	Problem with Console	The customer received an "Invalid Credentials" error when attempting to log in to the core GUI. Instead of logging in, they were taken to a screen displaying the error message along with a link.	3	23.2.0
37043384	OSO prom-svr crashing after CS-AMPCF/DB/ CNCC upgrade to 23.4.x	The OSO prom-svr failed after upgrading CS-AMPCF, DB, and CNCC to version 23.4.x.	3	23.4.0
37175346	IAM GUI cannot delete User Credentials	In the IAM GUI, the user was not able to delete the credentials.	4	24.2.0

> **Note**
>
> Resolved bugs from 23.4.3 and 24.2.1 have been forward ported to Release 24.3.0.

4.2.3 cnDBTier Resolved Bugs

Table 4-3 cnDBTier 24.3.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37468403	Cluster Failure observed in PCF microservices	Clusters failed in PCF microservices during MySQL cluster recovery. This issue is resolved by improving the MySQL cluster node recovery logic.	1	23.4.4
37163647	SR recovery issues	Issues were observed during system file maintenance and recovery.	2	24.2.1

Table 4-3 (Cont.) cnDBTier 24.3.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37447839	While upgrading the PVC value on 25.1.100-rc.2 dbtscale_vertical_pvc script is getting failed	The dbtscale_vertical_pvc script failed due to incorrect version number.	2	25.1.100
37448493	Seg. fault observed with ndbmtd while dbtpasswd change in progress	Segmentation fault was observed in the ndbmtd pods when cnDBTier password change was in progress.	3	25.1.100
37526391	Crash observed in data nodes during Installation	Data nodes crashed during installation due to segmentation fault in the ndbmtd pods when cnDBTier password change was in progress.	3	25.1.100
37527057	MTD pods restarted during upgrade from 23.4.2 to 25.1.100	MTD pods restarted during upgrade due to segmentation fault in the ndbmtd pods when cnDBTier password change was in progress.	3	25.1.100
37359397	occndbtier-24.3.0 db-monitor-svc is reporting multiple error logs with Non GR site	DB monitor service reported multiple error logs when there were no ndbmysqld pods in the cluster.	3	24.3.0
36142511	Heartbeat status returns 502 error code when accessed via CNDB sub-menu GUI and REST API for NRF	cnDBTier heart beat status API returned "502 Bad Gateway" response code in the ASM environment.	3	23.4.0
37404406	DBTier 24.2.1 helm rollback from TLS to non-TLS same version not dropping TLS	Rollback from a TLS enabled version to a non-TLS version failed.	3	24.2.1
37143214	All states of DR not displayed when DR triggered via dbtrecover	cnDBTier didn't display all states of georeplication recovery when the georeplication recovery was triggered using the dbtrecover script.	3	24.3.0

Table 4-3 (Cont.) cnDBTier 24.3.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37352523	Cndb tier 23.4 Helm chart does not pass Helm Strict Linting	Duplicate labels were generated for ndbmysqldsvc. As a result, users were unable to deploy cnDBTier Helm charts.	3	23.4.4
37442733	Helm test is failing on 25.1.100-rc.2	Helm test failed due to incorrect version of openssl during HTTPS certificate creation.	3	25.1.100
37601066	cnDBTier:24.2.x:snmp MIB Complain from SNMP server	cnDBTier SNMP MIB file did not support appending *.1* in the OID value.	3	24.2.0
37663827	cnDbTier 23.4.7 remote server private keys _permission issue	Permission issues were observed in the remote servers when private keys was set with the permission value of 600.	3	23.4.6
37308838	Correct the formula to calculate required pvc size in validatingresource stage	The formula to calculate the required PVC size in the validatingresource stage was incorrect.	3	24.3.0
37275946	Hikari connection pool warn message observed in db-monitor-svc logs	Hikari connection pool warning messages were observed in DB monitor service and DB replication service.	4	24.3.0
37272259	mysql-cluster-replication-svc logs continuous print of "SSLEngineImpl.java:825|Closing outbound of SSLEngine"	Duplicate SSL messages were observed in replication service logs.	4	24.3.0

Table 4-3 (Cont.) cnDBTier 24.3.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37401291	DBTier User Guide Needs update for BACKUP_SIZE_GROWTH alarm from 23.1.0	The backup size limit after which the BACKUP_SIZE_GROWTH alert is triggered was incorrectly mentioned as 5% instead of 20% in the cnDBTier user guide.	4	23.1.0

Table 4-4 cnDBTier 24.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
36939472	Data pods going into crash back loop off after restarting 2 data pods	Cluster failures were observed when graceful shutdown was performed on NDB nodes simultaneously within the same node group.	2	23.4.6
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
36750208	Replication down is observed for more than 10 mins during CNDB upgrade from 24.1.0 to 24.2.0-rc.3	Replication broke for more than ten minutes during cnDBTier upgrades. To resolve this, connection timeout was set for MySQL connection attempts in the db-replication-svc entry point script.	2	23.1.0
36725177	CNDB: 24.2.0-rc.3 crash being observed on db-monitor-svc	Issues were observed in DB monitor service pods due to Java heap memory size.	2	24.2.0
36921456	During CNDB TLS, HTTPS enabled upgrade, complete replication break is observed	Replication failed when performing an upgrade in TLS enabled deployments.	2	24.1.0

Table 4-4 (Cont.) cnDBTier 24.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
36909520	Pre-upgrade hook job fails on a setup deployed with pod and container prefix	Upgrade failed in ASM environment as there were empty container names when cnDBTier was deployed with container prefix.	2	24.2.0
36895369	cnDBtier Uplift : 23.1 to 23.3.1 - DR issue	cnDBTier didn't have separate TCP configurations for empty slot IDs used by the ndb_restore utility during georeplication recovery.	2	23.1.0
36795445	NRF- CNDBTier ndbappmysqld and db monitor service pods restarts observed with Exit Code 137	ndbappmysqld and DB monitor service pods restarted multiple times with exit code 137.	2	24.2.0
37191116	PCF DBTIER 24.2.1 Install - Error with template	cnDBTier installation failed as the Helm charts had an error in mysqld-configmap-data.tpl.	2	24.2.1
37214770	Standby replication channel went into FAILED state and didn't recover after restarting one management Dell switch	While adding a site, some ndbmysqld records were not inserted to the DBTIER_INITIAL_BINLOG_POSITION table after ndbmysqld pod scaling.	2	23.3.1
36613148	Avoid using occne-cndbtier pattern suggestion for DBTIER namespace examples due to OCCNE log ingestion filters	cnDBTier documents didn't clarify that the occne-cndbtier namespace name used in the documents is a sample namespace name and users must configure the name according to their environment.	3	23.3.1

Table 4-4 (Cont.) cnDBTier 24.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
36548525	DBTRecover stuck in waiting state	The dbtrecover script did not exit and got stuck in waiting state when georeplication recovery failed due to any reason.	3	24.1.0
36378250	Description is empty for health API when backup is not in progress	Description field within the backup manager service APIs was empty.	3	24.1.0
36660329	PCF DB 6 Replication - Users and Grants not replicated across sites	cnDBTier 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
36689742	During stage 2 of conversion misleading errors are observed	The conversion script displayed incorrect error messages during stage 2 and stage 3.	3	24.1.0
36779318	ndbmysqld pod is restarted with EXIT Code 2 during traffic run	Biglog purging logic failed to read decimal value when the disk size of ndbmysqld pods contained decimal numbers.	3	24.2.0
36555687	GR state is retained as "COMPLETED" when DR is re-triggered	The georeplication state was retained as "COMPLETED" when fault recovery was re-triggered using the dbtrecover script.	3	24.1.0
36753759	Alert: BACKUP_PURGED_EARLY not coming on prometheus	The BACKUP_PURGED_EARLY alert did not appear on Prometheus due to incorrect alert condition.	3	24.2.0

Table 4-4 (Cont.) cnDBTier 24.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
36482364	No RemoteTransferStatus displayed while the backup is being transferred from data pod to replication svc	Remote transfer status (RemoteTransferStatus) displayed incorrect value on Console GUI when backup transfer failed.	3	24.1.0
36742330	Automatic Backup fails to transfer files to remote host	Debug log options were not available for apscheduler, werkzeug, and paramiko.transport.sftp in the database backup executor service (db-backup-executor-svc) when logger mode was set to debug.	3	23.2.1
36492775	CNCC GUI does not show Service status as down for Backup Manager service when DB connectivity goes down with mysql pods in CNDB 24.1.0rc6	CNC Console GUI did not show service status as DOWN for the backup manager service when the database connectivity with MySQL pods got disconnected.	3	24.1.0
36961805	Cndbtier 22.4.2 db-monitor-svc pod got password security warn log	Password security warning logs were observed in database monitor service.	3	22.4.2
37058248	DB Tier metrics are missing for some times from the db-monitor-svc	cnDBTier metrics were missing from the DB monitor service as the system was unable to fetch the metrics from the database.	3	24.2.0
37078075	cnDBtier "Thread pool did not stop" errors log message	cnDBTier logs had the following unnecessary error message which had to be removed: "Thread pool did not stop"	3	22.4.2
37101586	Procedure to update vertical scaling for mgm pod should be documented	cnDBTier user guide didn't provide the procedure to scale the management pods vertically.	3	24.2.0

Table 4-4 (Cont.) cnDBTier 24.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37091194	DBTier 24.2.1 RestFuzz scan results flagged 500 (1) Response codes	cnDBTier RestFuzz scan displayed 500 error code for the get@/db-tier/purge/epoch/serverids/{serverIds} API.	3	24.2.1
37175416	Missing Alerts for NDBAPPMYSQLD or NDBMYSQLD	cnDBTier user guide didn't state that HIGH_CPU alerts are specific to data nodes.	3	23.4.4
36765073	When the connectivity between the Replication service and DB goes down, Replication service health status also showing as down on CNDB release 24.2.0rc3 build	The replication service health status was incorrectly displayed as DOWN when the connectivity between the replication service and DB went down.	4	24.2.0
36627536	dbtpasswd script accepts ampersand, but ampersand causes failure - please state in script help that ampersand not accepted	cnDBTier documentation missed information about the supported characters for database password.	4	23.2.0
36957553	NDBMGMD and NDBMTD container name not printed in pre and post upgrade hooks logs	ndbmgmd and ndbmtd container names were not printed in preupgrade and postupgrade hook logs.	4	24.2.1
37049002	Document cache/realtime time api details in DBtier user guide	cnDBTier API documentation didn't state whether the APIs provides real-time or cached data.	4	23.4.6
37144276	DBTier 24.2.1 Network policies - Incorrect pod selector for ndbmysqld	Incorrect pod selector was observed for ndbmysqld pods when network policy was enabled.	4	24.2.1

Note

Resolved bugs from 23.4.6, 24.1.2, and 24.2.2 have been forward ported to Release 24.3.0.

4.2.4 CNE Resolved Bugs

Table 4-5 CNE 24.3.3 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37842711	CNE installation fails in OL9	In the latest Oracle Linux 9 release, partitions were created differently. However, CNE cloud_growpart tasks required specific configuration. This resulted in bastions not having enough space to handle all their dependencies and configuration files leading to CNE installation failure.	4	25.1.100

Table 4-6 CNE 24.3.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37033023	Replacing a Controller node for CNE (CNLB based, version 24.2.0) giving error	The system ran into an error when a controller node was replaced in a CNLB based CNE.	2	24.2.0
37363771	CNLB ips not accessible in thrust3 cluster	CNLB IPs were not accessible causing the CNLB pods to restart frequently.	2	24.3.0
37435443	BM CNE 24.3.0: cnLB with VLAN segregration not working. cluster_test fails and no common services reachable	VLAN segregation in CNLB did not work. As a result, cluster_test failed and common services were unreachable.	2	24.3.0
37021718	After upgrade to 23.4.6 OCCNE still we are facing same issue reported in 23.4.4 lbvm pair is not taking traffic	The IP rule was missed during switchovers causing the traffic management to fail.	2	23.4.6
37398635	cnlb pods restarting on thrust3(24.3.0)	CNLB IPs were not accessible causing the CNLB pods to restart frequently.	3	24.3.0

Table 4-6 (Cont.) CNE 24.3.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37040679	vCNE opnstack upgrade failure with Local DNS enabled due to missing auto plugin config	When Local DNS was enabled, vCNE OpenStack upgrade failed due to a missing auto plugin configuration.	3	24.1.1

CNE 24.3.1 Resolved Bugs

There are no resolved bugs in this release.

Table 4-7 CNE 24.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36818112	CNLB Metrics pipeline stops to work after cnlb app pods logs starts throwing exception "ERROR in app: Exception on /metrics	CNLB metrics pipeline failed and metrics were not available when high volume of data was returned. This happened specially when CNLB application was running for a long time.	2	24.2.0
36958805	OCCNE 23.4.4 bastion failover not working with slow network speed to central repo	Bastion HA switchover failed due to slow image transfer speed from the CENTRAL_REPO host.	2	23.4.4
36843512	Cnlb app pods fails to configure network when network names do not end with numeric values on cnlb.ini file	CNLB application pods failed to configure network when network names were in the following format: "sig, sig2, sig3".	3	24.2.0

> **Note**
>
> Resolved bugs from 24.1.2 and 24.2.1 have been forward ported to Release 24.3.0.

OSO 24.3.1 Resolved Bugs

There are no resolved bugs in this release.

OSO 24.3.0 Resolved Bugs

There are no resolved bugs in this release.

4.2.5 NRF Resolved Bugs

Release 24.3.0

Table 4-8 NRF 24.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37184977	NRF uses the wrong error cod NRF uses the wrong error code when incoming gzip encoded content is received when incoming gzip encoded content is received	NRF rejected the incoming gzip encoded content request with 415 Unsupported Media Type indicating the supported encodings in HTTP requests, instead of responding with 400 Bad Request.	2	24.1.0
37174219	NRF sending "additionalAttributes" in NF subscription response is causing issues in AUSF/UDM	NRF was sending additionalAttributes in NFStatusSubscribe service operation response, which caused issues in AUSF or UDM.	2	23.4.4
37106652	Upgrade from 24.1.0 to 24.2.0 failed	NRF could not be upgraded from 24.1.0 to 24.2.0 as it was unable to start container and runc process was not able to access the docker-entrypoint.sh file on openshift. The file did not provide permission to other users to access it.	3	24.2.0
36802631	NRF - discovery response is sending incorrect Priority when no Preferred locality match for feature - NF Service Priority Update	NRF discovery response sent an incorrect Priority when there was no match in Preferred locality.	3	24.2.0
36823945	NRF - discovery response is sending incorrect P_Priority and S_Priority when Extended Preferred secondary locality NF profiles are not registered for feature - NF Service Priority Update	NRF discovery response sent an incorrect P_Priority and S_Priority when Extended Preferred Secondary Locality NF profiles were not registered.	3	24.2.0
36819966	NRF is sending 200 OK response for discovery request even when SLF query is failing and maxHopCount reached	NRF sent 200 OK response for discovery requests even when SLF query was failing and maxHopCount was reached.	3	24.2.0
36555795	When SLF and forwarding both feature are enabled, NRF is sending discovery response with NF Instances even when SLF is not reachable	When SLF and forwarding features were enabled, NRF sent discovery response with NF Instances even when SLF was not reachable.	3	24.1.0
36525061	NRF - nfdiscovery not sending Error response in correct format when Egress microservice not available	NRF nfdiscovery was not sending an error response in the correct format when the Egress microservice was down.	3	24.1.0
35963258	NRF- Inconsistent Error code in discovery response when forwarding enabled(200 Ok) and forwarding disabled(504) when no SLF is registered in NRF for feature - EXTENDED_DYNAMIC_SLF_SELECTION	NRF sent an inconsistent error code in discovery response when forwarding was enabled (200 Ok) and forwarding was disabled (504) when no SLF was registered in NRF for EXTENDED_DYNAMIC_SLF_SELECTION feature.	3	23.3.0

Table 4-8 (Cont.) NRF 24.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37184935	NRF includes accept-encoding header with value gzip in responses even though NRF doesn't support incoming gzip encoding content	NRF included accept-encoding header with value gzip in responses even though NRF doesn't support incoming gzip encoding content.	3	24.1.1
37184895	NRF-Alarm for inactive DbReplicationStatus	NRF triggered an alarm for inactive DbReplicationStatus.	3	23.4.4
36473305	NRF - detail parameter for Error code ONRF-CFG-ACCOPT-E0021 return invalid detail response	The detail parameter returned extra ":" in the error responses.	4	24.1.0
36720501	NRF Grafana Default Dashboard Gauge Failure, Incorrect Label, And Panel Questions	NRF Grafana Default Dashboard displayed Gauge Failure, Incorrect Label, and Panel Questions.	4	23.4.0
36683249	NRF - Incorrect format of detail parameter for Error ONRF-CFG-SCRNRUL-E0007	NRF was sending an incorrect format in detail attribute for the error code ONRF-CFG-SCRNRUL-E0007.	4	24.1.0
36684329	NRF - Incorrect Error Code ONRF-CFG-SCRNRUL-E0100 for cause MANDATORY_IE_MISSING	NRF was sending an incorrect error code ONRF-CFG-SCRNRUL-E0100 with the cause MANDATORY_IE_MISSING.	4	24.1.0

Table 4-9 NRF ATS 24.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37106545	Random regression test case failures	The test case failed as the wait time given in the test case between the registration of UDRs and validating the population of the slfDiscoveredCandidateList was the same as the refresh cycle of the slfCandidateList by nrfArtisan service. This caused random failures when the refresh cycle occurred (ms) before and after the given test case wait time.	3	24.1.2
37106677	NRF ATS - Regression test case failure	In OCC environment, the DNS server was taking a longer time to resolve incorrect FQDNs such as notifystub-service.atsnrf. Due to this, there are FT failures with timeout in Egress Gateway.	3	24.1.1

4.2.6 NSSF Resolved Bugs

NSSF 24.3.2 Resolved Bugs

Table 4-10 NSSF 24.3.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
38151570	500 Internal Server Error generated by NSSF (IGW) on GET request for nnssf-nsselection	The 500 Internal Server Error response was generated for the requests which has UserAgent header field with length more than 80.	3	24.3.0

NSSF 24.3.1 Resolved Bugs

Table 4-11 NSSF 24.3.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37636625	Inconsistencies seen when defining NSS rule with tac	The NSSF component was not displaying the TAC value in the NSS rule response when defined using the tac field. The issue was observed in CNDBTier, where the TAC was present in the nss_rule table but omitted in REST responses and CNC Console queries.	3	24.3.0
37651423	Subscribe Service Operation error pointing to missing supportedFeatures	NSSF was giving a 400 "BAD_REQUEST" error when trying to create a subscription using the nnssf-nssaiavailability service. This was happening because the supportedFeatures field was missing in the request, and the system was failing to handle it properly.	3	24.3.0

NSSF 24.3.0 Resolved Bugs

Table 4-12 NSSF 24.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
36823604	2-site GR setup ASM Enabled: Failover with overload : 15K TPS: while traffic reached to 15K(150% traffic), NSSF has dropped 13.9 percentage traffic with 500 error code and latency of ns-selection is 573 ms.	In a 2-site GR setup with ASM enabled, the NSSF component experienced significant issues under failover conditions with high traffic. When traffic scaled to 15K TPS (150% capacity), NSSF showed a high traffic drop rate and latency.	2	24.2.0
36872097	3-site GR setup ASM and Oauth Enabled: configure one slice on isolated site3 with ns-availability then after site3 recovery, Ns-Selection Get Request of that slice is getting error 403 FORBIDDEN on site-1 and site2	In a 3-site GR setup with ASM and OAuth enabled, NSSF encountered issues with Ns-Selection requests after a slice configuration and site recovery. When one slice was configured on an isolated Site-3 with ns-availability, Ns-Selection requests from Site-1 and Site-2 returned a 403 FORBIDDEN error after Site-3 restoration.	2	24.2.0
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.	During the upgrade of NSSF from version 23.2.0 to 23.3.0, there was a missing step in the documentation regarding the creation of a new database (nrf_client_db) and the required access permissions for this database.	3	23.3.0
36995282	NSSF is not including AMF details from AMF resolution table in candidate AMF list during NSSelection procedure response while whitelisted enable	When NSSF was performing an NSSelection procedure with whitelisting enabled, it did not include all candidate AMFs from the AMF resolution table in its response, resulting in an incomplete candidate AMF list. This affected subsequent AMF selection queries for the same slice, as the NSSelection response omitted AMFs that were part of the operator's configuration.	3	24.2.0
36879802	IGW/EGW Common Configurations Using CNCC GUI missing.	Documentation was missing for default configuration parameters in the NSSF 24.1.x User Guide and REST API Guide.	3	24.1.1

Table 4-12 (Cont.) NSSF 24.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
36907463	NSSF 24.1.1- Peer & PeerSet Default config with Relevant NF example and mode	Customer requests updates to the NSSF guide to clarify that configMode for SBI configuration only persists via REST, not HELM, and that definitions in CV YAML must be manually added to the database via CNCC/REST. They also want realistic examples for peerConfiguration and peerSetConfiguration fields in sbiRouting, using SCP virtual host values instead of ATS stub server defaults.	3	24.1.1
36625525	NSSF-CNCC: - Server header configuration done successfully without mandatory param	Configuration for the server header was completed successfully despite missing a mandatory parameter, which should have prevented it. This validation issue may affect other configuration parameters.	3	24.1.0
36633989	NSSF-CNCC: User agent header configured without mandatory param	User agent header configuration completed successfully without including nfInstanceId, a mandatory parameter.	3	24.1.0
36823225	Wrong error response title and DB (Auth & rule table) not cleared during the Availability update operation for White listed AMF.	During the Availability PUT and Subscription Modification processes, the response returns an incorrect string, and entries are not removed from the database as expected.	3	24.2.0
36817882	Auth & Rule table updated for Tailist and Tairange list for the slice which is restricted in Tai during NSAVailability update procedure for white list AMF but in response same is not coming.	The Auth & Rule table is incorrectly updated for a slice restricted in TAI during the NS Availability Update procedure for a whitelisted AMF. While the table updates correctly for the TaiList and TaiRangeList, the expected response does not reflect the correct configuration.	3	24.2.0

Table 4-12 (Cont.) NSSF 24.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
36777550	NSSF-FT : Error 500 with Internal Server error occurred while performed Availability delete for trusted AMF.	An Internal Server Error (500) occurs during the Availability Delete operation for a trusted AMF. The operation fails with an error indicating a database read/write error due to an overlapping tacrange, resulting in a moot configuration.	3	24.2.0
36662095	NSSF-CNCC : Ingress GW : Configuration param level as "Warning" missing from list for Overload control discard policy configuration	The configuration parameter level set as "Warning" is missing from the list for the Overload Control Discard Policy Configuration in the NSSF-CNCC Ingress Gateway documentation.	3	24.1.0
35971708	while pod protection is disabled, OcnssfIngressGatewayPodResourceStateMajor alert is not clear and resource metric is not updating to -1	While disabling Pod Protection, the OcnssfIngressGatewayPodResourceStateMajor alert is not cleared, leading to an incorrect view of resource status. Additionally, the resource metric fails to update to -1, while the congestion metric updates correctly.	3	23.3.0
36935312	NSSF does not include all supportedSnssaiLists in its subscription response which has present in DB	NSSF does not include all supportedSnssaiList entries in its subscription response, even though they are present in the database	3	24.2.0
35846922	Egress pod is not updating with the Entry done in DNS server "DNS SRV Based Selection of SCP in NSSF"	The Egress pod is not updating its entries based on changes made in the DNS server related to "DNS SRV Based Selection of SCP in NSSF.	3	23.3.0
35502848	Out of Range Values are being configured in PeerMonitoringConfiguration (Support for SCP Health API using HTTP2 OPTIONS)	Out of range values are being configured in the PeerMonitoringConfiguration for parameters such as timeout, frequency, failureThreshold, and successThreshold.	3	23.2.0

Table 4-12   (Cont.) NSSF 24.3.0 Resolved Bugs

Bug Number	Title	Description	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" & in notification msg	NSSF is not adding the User-Agent header in requests (Registration, Patch, Discovery, and Subscription) towards NRF when the configuration parameter overwriteHeader is set to false. The header is also missing in the notification message.	3	23.3.0
36817980	NSSF is sending Tacrangelist in response for NSAvailability procedure but not created in DB (Auth & Rule table) for NSAvailability procedure.	NSSF is sending the TAC range list in the response for the NSAvailability procedure, but it is not being created in the database during the NSAvailability procedure.	3	24.2.0
36926047	Error "tacrange encompassing the input tacrange is already present" occurred during the deletion of the ns-availability for one scenario.	An error, "tacrange encompassing the input tacrange is already present", is encountered when attempting to delete the ns-availability entry for a specific AMF. This occurs due to an overlap in tacrange configurations during NS availability updates, which leads to a database read/write error (DB_READ_WRITE_ERROR with status 500).	3	24.2.0
36949741	["AutoConfigurationFromNsAvailability":"Disable"] NSSF is sending an error response for ns-avail put with "No authorized Snssai found." when sst "200" is allowed in the database	NSSF returns a 403 Forbidden response with "No authorized Snssai found" when processing an ns-availability update request that includes sst: 200, despite this slice being allowed in the database (nssai_auth table). However, requests with other sst values, like sst: 254, process correctly and return a success response.	3	24.2.0
36662054	NSSF-CNCC: Ingress pod: Discard Policy mapping configured without mandatory param	An error arises in the NSSF-CNCC ingress pod due to a discard policy mapping that is missing a mandatory parameter.	3	24.1.0

Table 4-12 (Cont.) NSSF 24.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
36653405	Signature should validate for access token in non-asm setup	In a non-ASM (Application Service Management) setup, NSSF is expected to validate access tokens. However, when a token with a truncated signature (5 characters removed) is provided, the validation fails as expected, but the NSSF server does not respond with a precise cause, only indicating a general failure. This behavior contrasts with expected results from JWT validation tools (e.g., jwt.io), which correctly identify signature mismatches.	3	24.1.0
36838710	Multiple unsubscription happening while the initial unsubscription request sends 204 response	When a configured AMF Set is deleted, the NSSF initiates an unsubscription request to the NRF. Even when the unsubscription succeeds, the NSSF continues to retry, resulting in a 404 error (indicating the subscription was already deleted on the first attempt).	3	24.2.0
36814045	Slice entry created in Rule table during availability put procedure for the operator configured slice for Trusted AMF.	During the availability update (put) procedure for a trusted AMF, a slice entry is being created in the Rule table specifically for the operator-configured slice.	3	24.2.0
36756901	Bulk configuration and delete configuration API failing when DB has a large no of records	The bulk configuration and deletion of records in the amf_tai_snssai_map table are failing when handling large datasets, resulting in a 500 error code.	4	24.2.0
36966913	Metric Counter value given in User-Guide is not containing suffix total, which is present in Prometheus	Some of the metric counter values provided in the user guide do not include the suffix "total," while the corresponding metrics in Prometheus do contain this suffix.	4	24.2.0
36885942	Grafana Panels need to be updated or added for NSSF Grafana improvement	Improvements have been proposed for the NSSF Grafana dashboard to enhance monitoring capabilities and present data more effectively.	4	24.2.0

Table 4-12 (Cont.) NSSF 24.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
36882929	nfSetIdList is missing in the NSSF appProfile for NRF registration	The nfSetIdList parameter is absent from the NSSF application profile during registration with the NRF (Network Repository Function).	4	24.1.0
36829922	In Grafana NsSelection Overload Level Section, all types are shown in 3 times.	In the NSSF 24.2.0 Grafana snapshot, all types are displayed three times in both the NsSelection Overload Level and NsSelection Total Resource Overload Level sections.	4	24.2.0
36825575	OCNSSF 24.1.0 - CipherSuites config not exposed in custom value yaml file	Customers with strong security requirements need the ability to select specific cipher suites for the NSSF. Currently, these cipher suites are not exposed in the custom values YAML file, limiting customization based on internal or 3GPP security recommendations.	4	24.1.0
36407364	NSSF is displaying the error message for Failed to update Stats in the ocnssf performance pod.	The NSSF performance pod is encountering an error message stating "Failed to update stats" after the installation of the 24.1.0 release. This issue is disrupting the normal functioning of the NSSF.	4	24.1.0
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	During the in-service upgrade of NSSF from version 23.2.0 to 23.3.0 across two sites with ASM enabled, a noticeable increase in latency was observed: 228 ms at Site 1 and 237 ms at Site 2.	4	23.3.0
36943827	OCNSSF: The error details for the UnsupportedPLMN during Feature Negotiation are inaccurate.	When a request is made for a feature not supported by the NSSF, the error messages returned do not provide accurate or clear information regarding the supported features. This leads to potential confusion for users.	4	24.2.0

Table 4-12 (Cont.) NSSF 24.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
35986423	Both IGW pod protection and overload feature enabled, NSSF is not clearing the overload alerts when overload feature disabled in runtime.	The NSSF is not clearing overload alerts when the overload feature is disabled at runtime, despite both the Ingress Gateway (IGW) pod protection and overload feature being enabled initially.	4	23.3.0
37107033	NSSF 24.2.x - Missing Alerts In the User Documents	Several alerts listed in the alert rule files for versions 24.1.x and 24.2.x are missing from the user documentation. Undocumented Alerts: • OcnssfAuditorServiceDown • OcnssfAlternateRouteServiceDown • OcnssfNrfClientDiscoveryServiceDown • OcnssfNrfClientManagementServiceDown • OcnssfPerfInfoServiceDown • OcnssfOcpmConfigServiceDown	4	24.2.1
36634002	NSSF-CNCC : Peer monitoring configuration done successfully with provided Values "out of range"	The NSSF-CNCC peer monitoring configuration accepts values that are "out of range" for the timeout and frequency settings, indicating a lack of proper range validation.	4	24.1.0
35855937	In Ingress Gateway's Error Code Series Configuration, The names of the exceptionList and errorCodeSeries parameters are not verified.	The Ingress Gateway's Error Code Series Configuration does not validate the names of the parameters exceptionList and errorCodeSeries. As per NSSF REST Specification Guide, the NSSF should reject configurations with improperly named parameters.	4	23.3.0
36653053	NSSF-CNCC : Get key need to be removed from CNCC UI for "NSSF Restore" configuration since get functionality is not being supported for respective config param	The "Get" key for the "NSSF Restore" configuration should be removed from the CNCC UI, as the get functionality is not supported for this configuration parameter.	4	24.1.0

4.2.7 OCCM Resolved Bugs

Table 4-13 OCCM 24.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36915564	OCCM 24.2.0 helm test fail - Missing network policy	The Helm test was failing due to incorrect network policy version.	3	24.2.0
36925470	OCCM ConfigMap backup with latest build must be taken before rollback to older build as certificates/Issuers created with latest build can be restored if re-upgrade need to be done to latest build after rollback.	Use the OCCM ConfigMap backup with latest build before rollback to the older build. The certificates or issuers created with latest build can be restored if upgrade is perfomed to the latest build after rollback.	4	24.2.0

> **Note**
>
> Resolved bugs from 24.1.x have been forward ported to Release 24.3.0.

4.2.8 OCI Adaptor Resolved Bugs

Table 4-14 OCI Adaptor 24.3.0 Resolved Bugs

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

4.2.9 Policy Resolved Bugs

Table 4-15 Policy 24.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36681764	SM PCF CoSprings site was affected due to Memory utilization	SM service displayed timeout errors due to memory utilization issues.	1	23.2.7
36775172	Same session ID is triggered by PCF for different subscriber - Sd interface	Same session ID was triggered by PCF for different subscribers on Sd interface.	1	23.4.0

Table 4-15 (Cont.) Policy 24.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37197659	CNPCF 23.4.5 - SOS Call is not working when subscriber is in KDDI PLMN	For IMS and SOS APN, SOS call was getting failed, when subscriber was present in KDDI PLMN.	1	23.4.5
36884531	PCRF performance run observed Binding serv error "Invalid compressed data" & "No content to map due to end-of-input\n at [Source: (String)\"\";	Binding service de-register was failing with error "*Invalid compressed data*" and "*No content to map due to end-of-input\n at [Source: (String)*\"\".	2	24.2.0
36721504	cnPCRF 23.4.3 4G Reset Usage DataLimit action not working	In cnPCRF deployment, every time the usage limit reached 100% of usage quota, the data usage limit had to be manually reset.	2	23.4.3
36799692	Quota grants not considering float percentage values	Data usage quota grants did not consider floating percentage values.	2	23.4.3
36804006	cnPCF 23.4.0 // Egress GW removing IPv6 first hexadecimal Octet for N28 SpendingLimit request	Egress Gateway was altering the IPv6 address by removing the first hexadecimal octet, resulting in an invalid URL format.	2	23.4.0
36819053	BSF deregistration count came to zero after upgrading PCF to v23.4.3	After upgrading Policy from previous version to 23.4.3, binding deregistration did not happen (count became zero) from PCF. BSF deregistration details were not sent to BSF.	2	23.4.3
36560450	Multiple STR is triggered by cnPCRF towards OCS during performance testing	During race condition in Gx interface, cnPCRF initiated multiple Session Termination Requests (STRs) towards Online Charging System (OCS).	2	23.4.0

Table 4-15 (Cont.) Policy 24.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36674382	Post upgrade to 23.4.3, Policy Create, Policy Update and Policy Delete have error 403 Forbidden	After upgrading to 23.4.3, Ingress Gateway experienced 403 errors while processing SM CREATE, SM UPDATE, and SM DELETE requests. Also, UDR Connector encountered 403 error while processing Subscription request.	2	23.4.3
37198639	SMPCF - Policy Evaluation Failure	Policy Runtime Engine (PRE) displayed Policy evaluation errors due to missing Policy project.	2	23.4.6
37218156	PCF 24.2.x Bulwark POD creation error in ATS Lab with WS 1.5	Bulwark POD creation error was observed in ATS while installing or upgrading to Policy 24.2.1.	2	24.2.1
36909037	PRE performance degradation when using MatchList in Policy Table	PRE showed degradation in performance when a MatchList functionality was used with the Policy Table.	3	24.2.0

Table 4-15 (Cont.) Policy 24.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36724935	CnCP 24.1 Installation issue related to load balancer IP	There were issues while installing CNCP V24.1 in OCCNE V24.1. The load balancer IP was mentioned in the CNCP *custom-value.yaml* file as per NAPD sheet for services such as Config Management, Diameter Gateway, and Ingress Gateway. But, after installation, the service IP for Diameter Gateway was missing and the service IPs assigned for Config Management and Ingress Gateway were not correct in the yaml file.	3	24.1.0
36831526	Monitoring quota consume in a excess usage scenario - customer query	Currently, it is not possible to monitor the usage quota consumption when the data usage exceeds the limit.	3	23.4.0
36498769	PCF 23.4.0 Alerts not available in any of the MIB file for the Policy	Some of the alerts were missing in the MIB files, though they were mentioned in the Alerts rule files.	3	23.4.0
35843311	Do large policies impact performance?	Large policies impacted performance of PRE service.	3	23.2.2
36040853	PCF ENF_APP_Flow rule removal blockly not working	ENF_APP_Flow rule was not removed when the AF flow removal request was sent from PRE to PCRF Core as the ENF_APP_Flow rule removal blockly was not working.	3	23.2.4

Table 4-15 (Cont.) Policy 24.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36972096	Set Grant Volume blockly does not work when you use a dynamic variable and select bytes	Set Grant Volume blockly did not work in "Apply Data Limit Profile" when a dynamic variable was used to select bytes instead of selecting percentage.	3	22.4.7
36573839	PCRF not managing passes correctly	PCRF was not able to manage the passes that were controlling the expiration date and the consume status.	3	23.2.0
37235768	CHIO cnPCRF, POD restarted chio-cnp-cnpcrf-notifier	All the notifier pods were restarted at both the sites as per the chio-cnp-cnpcrf-notifier log.	3	23.2.8
36888364	Warning message "ProducerId Header is Not present in BSF Response"	There were multiple "ProducerId Header is Not present in BSF Response" warn logs in the binding pods.	3	23.4.4
36755773	SM-PCF sending nUDR subs-to-notify with two monitoredResourceURIs in the message - resulting in N36 setup failure	SM-PCF was sending nUDR subs-to-notify with two monitoredResourceURIs in the message resulting in N36 setup failure.	3	23.4.3
36474704	Diameter message latency Metrics	The diameter message latency metrics were missing.	3	23.4.0
37081363	Usage-monitoing pod logs are not included in the Subscriber activity log	Usage monitoring pod logs were not included in the subscriber activity log.	3	23.4.3
36919835	SCP alert for occnp does not work	The SCP_PEER_SET_UNAVAILABLE alert was getting falsely triggered due to wrong expression.	3	23.4.0

Table 4-15 (Cont.) Policy 24.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36666113	Alert Queries for 23.4 documentation	Some of the alerts did not have appId filter in the expression.	3	23.4.0
36785603	pcf01cro perf-info generating multiple "MYSQL_OPT_RECONNECT"	The Perf-info service was generating multiple "*MYSQL_OPT_RECONNECT*" errors.	3	23.4.3
36820314	pcrf-core generating "exception when calculating the maxRuleNumber" errors	The PCRF Core service was generating "*exception when calculating the maxRuleNumber*" error during deployment.	3	23.4.3
36924410	QOS parameter : Max DataBurstVol" is taking values between 1-4065 and not 0 or null	The QOS parameter "Max DataBurstVol" was not taking 0 or null value.	3	24.1.0
37141274	Configuration Updates using Helm / Documentation Update	The configuration updates were not working during in-service Helm upgrade.	3	22.4.7
36785839	PCF sending incorrect NCGI format in Rx RAR to CSCF	PCF was sending incorrect NCGI format in Rx RAR to CSCF.	4	23.4.0
36817640	SM PCF egress traffic failing after 23.4.2 Upgrade	SM PCF egress traffic was failing after the upgrade to 23.4.2.	4	23.4.2
36817660	PCF AM-001 EGW 503 ERRORS	While sending on demand discovery request, NRF-Client was sending an empty data frame in addition to the GET request.	4	23.4.3
36643981	All Data Limit Profiles are sent to the PRE microservice	All data limit profiles were sent to the PRE microservice.	4	23.4.3
37097440	Huge logs are flooding as "Exit requested from Policy evaluation" due to end all blockly	There were multiple logs with "Exit requested from Policy evaluation" message due to End All blockly.	4	22.4.4

Table 4-15 (Cont.) Policy 24.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37060159	CNC Policy 23.4.5 - STR is not sent by PCF if CCA-I sent with error code	PCF was not sending session termination (STR) request when it was sending error code in Credit-Control-Answer (CCA-I) towards Packet Gateway (PGW).	4	23.4.5

Note

Resolved bugs from 24.2.1 and 24.2.2 have been forward ported to Release 24.3.0.

Table 4-16 Policy ATS 24.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37228249	CF-ATS 24.2.1 - NRF_Error_Response_Enhancement_PCF_as_Producer failure in NewFeature (24.3.0)	The scenario "NRF_UDR_Register_and_Suspension" from "NRF_Error_Response_Enhancement_PCF_as_Producer" new feature was failing.	3	24.2.1

4.2.10 SCP Resolved Bugs

Table 4-17 SCP 24.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37004532	SCP 24.2.0: Mediation not working when Target NF is known by SCP	In SCP 24.2.0, Mediation did not work when the target NF was known by SCP.	2	24.2.0
37078504	SCP CPU Utilisation shows parameters unexpected values on grafana dashboard for some of the pods	SCP CPU utilization displayed unexpected values of some parameters on the Grafana dashboard for some of the pods.	3	24.2.1
37013969	Scraping of grafana metrics needs to be fine tuned	In the 730K MPS duration of 60 hours, a few metrics were scraped on the Grafana dashboard.	3	24.2.1

Table 4-17 (Cont.) SCP 24.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34888941	Description of values/ paremeters used in SCP queries missing from User Guide or REST SPEC Doc	Descriptions of some of the REST API parameters and values required modification in the Oracle Communications Cloud Native Core, Service Communication Proxy RESTSpecification Guide.	3	22.3.2
36657810	SCP: On configuring private & public key with same name under rsa and ecdsa section and selecting algorithm as "ES256" then scp-worker pod is not coming up when TLS is enabled.	After configuring private and public key with the same name under the RSA and ECDSA section and selecting algorithm as "ES256," SCP-Worker pod did not come up when TLS was enabled.	3	24.1.0
36969335	SCP should not forward internal hop traffic to OCNADD	SCP should not have forwarded internal hop traffic to Oracle Communications Network Analytics Data Director (OCNADD).	3	23.4.0
36969322	SCP hop-by-hop-id metadata in messages forwarded to OCNADD should be unique for messages in each hop	SCP's hop-by-hop-id metadata did not have a specific format to identify requests and responses forwarded to OCNADD.	3	23.4.0
36932908	Some CNCC GUI Parameters missing for System Config Options	Some CNC Console fields were missing for System Config options.	3	23.4.3
36827133	Jaeger transaction correlation for internal messages missing.	Jaeger transaction correlation for internal messages was missing.	3	23.4.1
36765928	OCSCP: Missing Metrics Release 23.4.0	The ocscp_metric_http_tx_res_total metric was incorrectly documented in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.	3	23.4.0
36757271	Readiness_failure observed for 2 worker pods during the upgrade from 24.1.0 to 24.2.0-rc.5 image	Readiness_failure was observed for two SCP-Worker pods during the upgrade from 24.1.0 to 24.2.0-rc.5 image.	3	24.2.0
36730955	"NF Rule Profile Data" filter is not functioning properly, which will affect the analysis of data with a large number of NF profiles configured on SCP	The NF Rule Profile Data filter was not functioning, which affected the analysis of data with a large number of NF profiles configured on SCP.	3	24.2.0
36698507	TLS Handshake fails intermittently with TLS version 1.3 after idle timeout	TLS handshake failed intermittently with TLS version 1.3 after idle timeout.	3	24.2.0

Table 4-17 (Cont.) SCP 24.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36697266	SCP Serving scope info is missing in NF Rule Profile Data in Console GUI	SCP Serving scope info was missing in NF Rule Profile Data on the CNC Console.	4	24.2.0
36610824	service level routing options is not getting updated when we remove resource_exhausted from exceptionErrorResponses by enabling enhanced error response	The service level routing options were not updated when resource_exhausted was removed from exceptionErrorResponses by enabling enhanced error response.	4	24.1.0
36357539	Error message for NF Profile configuration Capacity is miss leading	When an incorrect value was configured for Capacity for a registered NF Profile, SCP responded with an invalid error range instead of a valid error range.	4	23.4.0
36013206	Some Attribute needs correction in ocscp_metric_http_tx_total and ocscp_metric_http_rx__total when Message Type is CALLBACK or NOTIFICATION REQUEST.	Some attributes required correction in ocscp_metric_http_tx_total and ocscp_metric_http_rx__total metrics when the Message type was CALLBACK or NOTIFICATION REQUEST.	4	23.3.0
36979853	Configuration guidance needed for Circuit Breaking feature	Documentation gaps related to feature configuration were identified for some of the legacy features, such as Circuit Breaking.	4	23.4.3
36915264	Default value of log rate needs to modified for scp-worker	The default value of log rate was not modified for SCP-Worker.	4	24.2.0
37026907	Missing info for Pod Overload Control feature	Some information was missing in the Pod Overload Control feature description of the Oracle Communications Cloud Native Core, Service Communication Proxy User Guide.	4	23.4.3
37461577	Irrelevant metrics of reactor netty and common Jar getting pegged in worker and other services of SCP	Irrelevant metrics of reactor netty and common Jar were pegged in SCP-Worker and other services of SCP.	4	24.2.0

> **Note**
>
> Resolved bugs from 24.1.2 and 24.2.1 have been forward ported to Release 24.3.0.

4.2.11 SEPP Resolved Bugs

Table 4-18 SEPP 24.3.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37669351	Need assistance to test Health Check Feature.	Health monitoring was enabled on one Remote SEPP, but no GET messages were seen on the Egress Gateway. This was because the prepareScheduler() method had not cleaned up existing scheduled tasks before starting new ones. As a result, multiple health check tasks were created and run concurrently, which increased the SCP health check request rate.	3	24.3.1
37897269	Failure of proactive status update feature ATS cases.	The Proactive status update feature ATS cases were failing with the default configuration. This was because the health status metric (oc_egressgateway_peer_health_status) was updated after 9 seconds (3 second frequency × 3 [failure/success threshold]). However, the ATS was configured to check the value of this metric in less than 9 seconds. The *Cloud Native Core Automated Testing Suite Guide* is updated to instruct setting peerMonitoringConfiguration.failureThreshold: 1 and peerMonitoringConfiguration.successThreshold:1 in the ocsepp_custom_values_<version>.yaml file before running the ATS suite.	3	24.3.2

Table 4-19 SEPP 24.3.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37543709	SEPP is changing nsmf-pdusession Encapsulated multipart: Message type: to Unknown (0xef)	It was observed that when a multipart message was received or sent by SEPP, the message was corrupted at Ingress Gateway or Egress Gateway and 'Message type: Unknown (0xef)' was observed on SEPP services.	2	24.3.0

Table 4-20 SEPP 24.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36767431	Call failed observed with error code 500,503,504,408 during and n32-ingress-gateway restart with 137-Error code during 56K MPS performance run with Cat3 feature enabled with cache refresh time 120000 at sepp_24.2.0-rc1.	Traffic issues were noticed with the Gateway 24.2.x releases, which caused an IllegalReferenceCount exception when the Cat-3 feature was enabled.	3	24.2.0
36777756	Call failed observed with error code 500,503,504,408 during 56K MPS performance run with SOR feature enabled at sepp_24.2.0-rc1.	Traffic issues were noticed with the Gateway 24.2.x releases, which caused an IllegalReferenceCount exception when the SOR feature was enabled.	3	24.2.0
37134044	Detailed IP/Service Flow	The confluence page in which detailed IP and service Flow for SEPP is to be created.	3	24.2.0
37046531	SEPP Call failures with 4xx & 5xx Error codes with 24K MPS traffic with message copy.	There were call failures with 4xx and 5xx error codes. Each SEPP site handled 24K MPS of traffic, and MessageCopy traffic was also at 24K MPS toward Oracle Communications Network Analytics Data Director (OCNADD). After running SEPP overnight for 12 hours, it was observed about a 1.7% call drop due to the error codes.	3	24.2.0

Table 4-20 (Cont.) SEPP 24.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
34374452	SCP-SEPP_FT: Residue pending in DB after deleting 900 RS created	When the pn32c and cn32c pods were scaled down, a delete request raised for a configured remote SEPP returned a 204 response, but the entry was not deleted. Additionally, no error was displayed when a POST request was executed while the pods were scaled down. This issue was observed when a script was run to add and delete 900 remote SEPPs, resulting in a race condition.	3	22.2.0
36897010	SEPP Topology Hiding does not support Multipart message type	The multipart message type was not supported by the SEPP Topology Hiding feature.	3	23.4.0
36616858	call failed with error code 500,503,504,408 observed during 56K MPS performance run with topology Hiding, SCM(Cat0,Cat1,Cat2,Cat3),Overload, Mediation, SOR, RateLimiting feature enabled.	The traffic issues were observed with the Gateway 24.2.x releases and are getting an IllegalReferenceCount exception when the security features were feature is enabled.	3	24.1.0
36749086	OCI Alarms utility 24.2.0 package for zip has not released and we are using the 24.1.0 zip package	The OCI alarms utility package for version 24.2.0 was not released, hence SEPP was using version 24.1.0.	3	24.2.0
36666519	Producer/Consumer FQDN contain ":port" while messageCopy is enabled on GWs	For the header 3gpp sbi api root '3gpp-sbi-target-apiroot': 'http://RJBAR.UDCVMH.HSS02.UDM.5gc.mnc011.mcc724.3gppnetwork.org:8080'}. The FDQN had port, but, the FQDN (both producer and consumer) should not contain the port as per 3GPP specifications.	4	23.4.0
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 values were observed when the Alternate Routing feature was enabled.	4	23.3.0

Table 4-20 (Cont.) SEPP 24.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37026047	Support for "mysql_native_password" plugin deprecated by CNDB	cnDBTier deprecated support for the "mysql_native_password" plugin and must use the "caching_sha2_password" plugin instead. This change had to be reflected in the *Cloud Native Core, Security Edge Protection Proxy Installation, Upgrade, and Fault Recovery Guide*.	4	24.2.0
36924956	Unable to exit the options screen without selecting "Supported Header Name"	In the SEPP section of the CNC Console GUI, on the Originating Network ID Header support options page, users were unable to click the cancel button without selecting a supported header name, as it was set as mandatory.	4	24.2.0
36824145	content-type is application/json instead of application/problem+json in case of cat3 failure generated by pSEPP	While running a failure scenario for Cat-3 feature (when the UE was not authenticated), it was observed that the content type should have been "application/problem+json" instead of "application/json."	4	24.2.0
36577733	oc_ingressgateway_incoming_tls_connections metric counter coming in -ve	The value of oc_ingressgateway_incoming_tls_connections metric count was -1 in Prometheus.	4	24.1.0

ⓘ **Note**

Resolved bugs from 24.2.0 and 24.2.1 have been forward ported to Release 24.3.0.

4.2.12 UDR Resolved Bugs

Table 4-21 UDR 24.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37003391	After Running performance for 72 hrs UDR Stopped sending PNRs and error observed in Notify service.	UDR stopped sending Push Notification Request (PNR) after 72 hours of performance run and erros were observered in the notify service.	2	24.2.0
36094811	Migration tool performance issue to read records from 4G UDR at high TPS	There was performance issue in the migration tool in reading the records from 4G UDR at high Transaction per Second (TPS).	3	23.4.0
36810163	Sender value in the Notify-service error log should be same as server header value sent by Egressgateway	The value in the notify service error log was not same as the server header value sent by Egress Gateway.	3	24.2.0
36829216	UDR is sending Multiple Resources under "delResources" parameter in notification of subscriber deletion	UDR was sending multiple resources with delResources parameter in the notification of subscriber deletion.	3	24.2.0
36998857	SLF- In oso alert file for SLF severity for all alerts is same in overload scenario	The severity of all the alerts in an overload scenario was same in OSO alert yaml file for SLF.	3	24.2.0
36886192	PROVGW installation is failing when ndb_allow_copying_alter_table: 'OFF' in DBTIER yaml file	The Provisioing Gateway installation was failing when ndb_allow_copying_alter_table is set to OFF in cnDBtier yaml file.	3	24.2.0
36879860	UDR 24.2.0 - Enhanced Error Logging not capturing the 500 error details for nudr-dr-prov service	The Enhanced Error Logging feature was not capturing the 500 error details for nudr-dr-prov service.	3	24.2.0
36878728	UDR 24.2.0 - Log throttling configuration not complete for diam-gateway service in cv file	The log throttling rate configuration was not available for the diam-gateway service in the custom value file.	3	24.2.0
36872918	Diameter Gateway Congestion cannot be disabled from CNCC GUI	The diameter gateway congestion control could not be enabled or disabled from CNC Console.	3	24.2.0

Table 4-21 (Cont.) UDR 24.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36871318	Error "Error Code: 400] - commonconfig: Could not find the config for requested service instance.: CCS-E107 - BAD_REQUEST" observed while adding the Route configuration through console, but through rest API its working successfully.	When adding or updating the route configuration through CNC Console, the addition was failing with Error Code: 400. The configuration for the requested service instance were not found.	3	24.2.0
36813453	During Performance for Call Model 1- 25K SH Traffic drops to 15K SH.	The Diameter SH traffic was dropping from 25k to 15K during Performance Call Model for 25K Diameter SH traffic.	3	24.2.0
34745401	User Agent Header is present in UDR EGW messages even when configuration flag is set to false	User Agent Header was present in UDR egress gateway messages even when the configuration flag was set to false.	3	22.3.1
37036000	UDR TLSv1.3 Support - Ingress TLS Metric getting populated with negative values	Negative values were populated in Ingress TLS metric.	3	24.2.0
37017032	SLF- As per user document we are not able to modify the parameter sftpDetails.enable in bulk-import with console and rest api	Unable to modify the sftpDetails.enable parameter in bulk-import using CNC Console and REST API.	3	24.2.0
36841691	UDR 24.2.0 - Observed Multiple Error Logs for nudr-dr service	Multiple error logs were observed for nudr-dr service.	4	24.2.0
36814613	Subscriber trace message for Failure is incorrect for 400 Failure response of POST Request	For the Post request, the subscriber trace message for failure was incorrect for 400 failure response.	4	24.2.0
36326798	Supi range format in AppProfile section in UDR YAML is in invalid format[12 digits]	The format of the Subscription Permanent Identifier (SUPI) range was invalid in the app profile section of the UDR yaml file.	4	23.4.0
37009619	SLF specific Metrics needs better clarification	Metrics specific to SLF needed more information.	4	24.1.0
36841691	UDR 24.2.0 - Observed Multiple Error Logs for nudr-dr service	Multiple error logs was observed for nudr-dr service.	4	24.2.0

ⓘ **Note**

Resolved bugs from 24.2.1 have been forward ported to Release 24.3.0.

4.2.13 Common Services Resolved Bugs

4.2.13.1 ATS Resolved Bugs

Table 4-22 ATS 24.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
36929173	Wrong rerun count considered for applogs when similar stage names are available	An incorrect rerun count was considered for applog file names when similar stage names were available.	4	24.3.0
37021232	While calling one tag based scenario using ATS API, Stage hooks are running for all the stages	When calling a tag-based execution using the ATS API, stage hooks ran for all stages instead of only those related to the selected tags.	4	24.3.0

Note

Resolved bugs from 23.2.1 have been forward ported to Release 24.3.0.

4.2.13.2 ASM Configuration Resolved Bugs

Release 24.3.0

There are no resolved bugs in this release.

4.2.13.3 Alternate Route Service Resolved Bugs

Release 24.3.0

There are no resolved bugs in this release.

4.2.13.4 Egress Gateway Resolved Bugs

Table 4-23 Egress Gateway 24.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36855523	Message Copy Support At EGW-Query parameter is striped out from path header while copying data to DD	The query parameter was stripped out of the path header while copying data to OCNADD.	3	24.2.3

Table 4-23 (Cont.) Egress Gateway 24.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36459166	IGW Helm Charts does not pass YAML Lint check	Helm charts did not pass the strict YAML Lint check.	3	24.1.0

> **Note**
>
> Resolved bugs from 24.1.x have been forward ported to Release 24.3.0.

4.2.13.5 Ingress Gateway Resolved Bugs

Table 4-24 Ingress Gateway 24.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
36800906	PCF sending error 415(UNSUPPORTED_MEDIA_TYPE) when policyauthorization delete request is being received without content-type header	After integration with E// NEF, E// NEF sent a Delete POST HTTP2 message with the Content-Type header. PCF (Ingress Gateway) rejected this message with a 415 error (unsupported media type).	3	23.1.4

> **Note**
>
> Resolved bugs from 24.1.x have been forward ported to Release 24.3.0.

4.2.13.6 Common Configuration Service Resolved Bugs

Release 24.3.0

There are no resolved bugs in this release.

4.2.13.7 Helm Test Resolved Bugs

Release 24.3.0

There are no resolved bugs in this release.

4.2.13.8 App-Info Resolved Bugs

Release 24.3.0

There are no resolved bugs in this release.

4.2.13.9 NRF-Client Resolved Bugs

Table 4-25 NRF-Client 24.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36942169	NRF-Management pod is reporting "Possibly consider using a shorter maxLifetime value	NRF-management pod is reporting continuous WARN Possibly consider using a shorter maxLifetime value.	3	24.2.1

4.2.13.10 Perf-Info Resolved Bugs

Release 24.3.0

There are no resolved bugs in this release.

4.2.13.11 Debug Tool Resolved Bugs

Release 24.3.0

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

Table 4-26   BSF 24.3.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36912994	BSF Diam-gw throwing DOC warning when congestion is not enabled	BSF Diameter Gateway is throwing Danger Of Congestion (DOC) warning when congestion is not enabled.	There is no functional impact as congestion warnings are logged even though the congestion feature is not enabled. **Workaround**: Set appropriate configuration in the custom-values.yaml file by providing the following list of headers, which do not require indexing: headerIndexing: doNotIndex:	3	24.2.0

ⓘ **Note**

Known bugs from 24.1.x and 24.2.x have been forward ported to Release 24.3.0.

4.3.2 CNC Console Known Bugs

CNC Console 24.3.0

There are no known bugs in this release.

4.3.3 cnDBTier Known Bugs

Table 4-27 cnDBTier 24.3.1 Known Bugs

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

Table 4-28 cnDBTier 24.3.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37135914	DBTIER 24.2.1 : DBTier down during CNE upgrade (K8S stage)	cnDBTier cluster goes down while performing a CNE upgrade (Kubernetes stage).	cnDBTier cluster goes down while performing an upgrade and the cluster must to be restarted manually. **Workaround**: Perform the following steps to recover the cnDBTier cluster by restarting ndbmtd-0 with the --initial flag: 1. Restart all the data pods. 2. Delete ndbmtd-0 a couple of times such that its initialization doesn't progress. This is necessary as Kubernetes starts the pods in order and it doesn't start the next pod until the previous pod is running and READY. The objective here is to bring up the other pods without ndbmtd-0 and restart them all before deleting the PVC of ndbmtd-0. 3. When the other pods are up, delete the PVC and the pod for ndbmtd-0. 4. When the above steps are done, the system automatically copies the database for ndbmtd-0 from ndbmtd-1 and the cluster comes up.	2	24.2.1

Table 4-28 (Cont.) cnDBTier 24.3.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36487409	dbtpasswd doesn't retain the old password in some of the pods	The dbtpasswd script doesn't retain the old password in some of the pods.	While using the dbtpasswd script, application pods with old password may not be able to connect to cnDBTier database. The connection of application pods depends on the mysqld pod that is used to attempt the connection with cnDBTier database. If the mysqld pod is one of the affected pods, then the connection fails. **Workaround**: Restart the application pods with the old passwords, so that the pods get the new password from Kubernetes secret.	3	23.4.2
36665039	Replication Went Down during NEF DBTier Upgrade from v23.4.3 to 24.2.0-rc.1	Georeplication fails in NEF during a cnDBTier upgrade from 23.4.3 to 24.2.0.	NEF georeplication fails with remote cnDBTier clusters. This requires you to perform georeplication recovery procedures to restore the georeplication with remote cnDBTier clusters. **Workaround**: Divert the NEF traffic from the current cnDBTier cluster to other remote cnDBTier clusters and then perform the upgrade of the current cnDBTier cluster. Repeat the same approach to upgrade other remote cnDBTier clusters.	3	24.2.1

Table 4-28 (Cont.) cnDBTier 24.3.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release

37308838	Correct the formula to calculate required pvc size in validatingresource stage	The formula to calculate the required PVC size during a georeplication recovery is incorrect in the replication service.	If /db-replication-svc/validateresourcesingeorecovery is enabled, the leader replication service will expect more PVC size during a georeplication recovery in the VALIDATERESOURCES stage and the georeplication recovery might fail.
			Workaround:
			Add the following parameter to the /global/ndb/ section of the custom_values.yaml file before installing or upgrading cnDBTier:
			`global:`
			`  ndb:`
			`    ndbbackuppercentagefordatamemory: 24`
			This parameter provides the maximum size of the backup with respect to the percentage of data memory and is used to calculate the expected backup size per data node during georeplication recovery. The value of this parameter must be set to *24* if /db-replication-svc/validateresourcesingeorecovery is set to *true*.
				3	24.3.0

4.3.4 CNE Known Bugs

Table 4-29 CNE 24.3.3 Known Bugs

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

Table 4-29 (Cont.) CNE 24.3.3 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release

37564804	pipeline.sh failing with 24.3.2 CNE version	The pipeline.sh script fails with the error, "ERROR: Can not delete output file : No such file or directory" during Bare Metal installation.	BareMetal installation fails.
			Workaround:
			Perform the following steps:
			1. a. Run the following `export` command on the `provision.yaml` file as a workaround.
			Note: This is applicable for BareMetal installation only.
			`podman run -v $PWD:/target occne/provision:24.3.2 cp /provision/provision.yaml /target`
			`# Verify the line`
				2	24.3.2

Table 4-29 (Cont.) CNE 24.3.3 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
			65 in provision.yaml, if indentation is correct after executing below line sed -i '65i\ serial=1' provision.yaml export OCCNE_PROV_PODMAN_DEPLOY_ARGS=' -v $PWD/provision.yaml:/provision/provision.yaml' 2. Rerun the pipeline.sh script or deploy.sh script depending on which step being performed, that is, bootstrap or first bastion.		

Table 4-29 (Cont.) CNE 24.3.3 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release

37552439	pipeline.sh fails with error in cosmos cluster(baremetal with cnlb)	The pipeline.sh script fails with the error, "ERROR: Can not delete output file : No such file or directory" during Bare Metal installation.	BareMetal installation fails.
			Workaround:
			Perform the following steps:
			1. a. Run the following `export` command on the `provision.yaml` file as a workaround.
			Note: This is applicable for BareMetal installation only.
			`podman run -v $PWD:/target occne/provision:24.3.2 cp /provision/provision.yaml /target`
			`# Verify the line`
				2	24.3.2

Table 4-29 (Cont.) CNE 24.3.3 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
			65 in provision.yaml, if indentation is correct after executing below line sed -i '65i\ serial=1' provision.yaml export OCCNE_PROV_PODMAN_DEPLOY_ARGS=' -v $PWD/provision.yaml:/provision/provision.yaml' 2. Rerun the pipeline.sh script or deploy.sh script depending on which step being performed, that is, bootstrap or first bastion.		

Table 4-30 CNE 24.3.2 Known Bugs

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

Table 4-30 (Cont.) CNE 24.3.2 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release

37564804	pipeline.sh failing with 24.3.2 CNE version	While installing a BareMetal CNE, the pipeline.sh script fails with the following error: "ERROR: Can not delete output file : No such file or directory"	BareMetal CNE installation fails.
			Workaround:
			Perform the following steps while installing a BareMetal CNE:
			1. Run the following command to get the updated provision.yaml file:
			`podman run -v $PWD:/target occne/provision:24.3.2 cp /provision/provision.yaml /target`
			2. Verify if the indentation in line number "65" is correct:
			`sed -i '65i\ serial=1' provision.yaml`
			3. Run the following comman
				2	24.3.2

Table 4-30 (Cont.) CNE 24.3.2 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
			d to set the environment to use the updated provision.yaml file: `export OCCNE_PROV_PODMAN_DEPLOY_ARGS=' -v $PWD/provision.yaml:/provision/provision.yaml '` **Note:** The workaround must be performed on the Bootstrap before running the deploy.sh script and then on the first Bastion before running the pipeline.sh script. After performing the workaround, rerun the pipeline.sh or deploy.sh script depending on the installation step you are in.		

Table 4-30 (Cont.) CNE 24.3.2 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release

37552439	pipeline.sh fails with error in cosmos cluster(baremetal with cnlb)	While installing a BareMetal CNE, the `pipeline.sh` script fails with the following error: `"ERROR: Can not delete output file : No such file or directory"`	BareMetal CNE installation fails.
			Workaround:
			Perform the following steps while installing a BareMetal CNE:
			1. Run the following command to get the updated `provision.yaml` file:
			`podman run -v $PWD:/target occne/provision:24.3.2 cp /provision/provision.yaml /target`
			2. Verify if the indentation in line number "65" is correct:
			`sed -i '65i\ serial=1' provision.yaml`
			3. Run the following comman
				2	24.3.2

Table 4-30 (Cont.) CNE 24.3.2 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
			d to set the environment to use the updated provision.yaml file: `export OCCNE_PROV_PODMAN_DEPLOY_ARGS=' -v $PWD/provision.yaml:/provision/provision.yaml '` **Note:** The workaround must be performed on the Bootstrap before running the deploy.sh script and then on the first Bastion before running the pipeline.sh script. After performing the workaround, rerun the pipeline.sh or deploy.sh script depending on the installation step you are in.		

CNE 24.3.1 Known Bugs

There are no new known bugs in this release. For existing known bugs, see "CNE 24.3.0 Known Bugs".

Table 4-31 CNE 24.3.0 Known Bugs

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

Table 4-31 (Cont.) CNE 24.3.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37191805	OL9 UEKR7 channel iproute-6.8.0-1.el9_4.x86_64.rpm triggers egress-controller CrashLoopBackoff	After an OS update, all CNE egress controllers are stuck in CrashLoopBackoff as the new IP route RPM saves the rt_tables file in an incorrect file path.	Egress service gets impacted. **Workaround**: Perform the following procedure to manually add the rt_tables file on the host of the egress controllers: **Note:** Run all the commands from the active Bastion Host. 1. Create the rt_tables file in the cluster directory with the following content: # # reserved values # 255 local 254 main 253 default 0 unspec # # local # #1 inr.ruhep 2. Create the updRtTables.sh script in	2	24.1.1

Table 4-31 (Cont.) CNE 24.3.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release

			the cluster directory:
			`#!/bin/bash`
			`occne_all.sh 'mkdir -p /etc/iprotue2' kube-node`
			`for worker in $(kubectl get nodes | grep k8s-node | awk {'print $1'}); do`
			`  scp -i .ssh/occne_id_rsa.pub /var/occne/cluster/${OCCNE_CLUSTER}/rt_tables  cloud-user@${worker}:/etc/ipropute2/rt_tables`
			`done`
			3. Change the permissions for the		

Table 4-31 (Cont.) CNE 24.3.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release

			new script to executable:
			`chmod 777 /var/occne/cluster/<cluster_name>/updRtTables.sh`
			4. Run the script from the cluster directory:
			`/var/occne/cluster/<cluster_name>/updRtTables.sh`
			5. Run following commands to restart the egress controllers and ensure that all controller are up running:
			`$ kubectl rollout restart ds occne-`		

Table 4-31 (Cont.) CNE 24.3.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release

			egress-controller -n occne-infra
			$ kubectl rollout status ds occne-egress-controller -n occne-infra
			$ kubectl get pods -n occne-infra | grep occne-egress-controller		

OSO 24.3.1 Known Bugs

There are no known bugs in this release.

OSO 24.3.0 Known Bugs

There are no known bugs in this release.

4.3.5 NRF Known Bugs

Table 4-32 NRF 24.3.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36998663	NRF Call Success Rate Drops During OCCNE Solution Upgrade from 23.4.5 to 24.1.1	NRF call success rate drops during OCCNE solution upgrade from 23.4.5 to 24.1.1.	Traffic loss occurred when the worker nodes were drained and pods were rescheduled to new worker nodes. Traffic loss becomes zero only after rescheduling of all the NRF pods is completed. **Workaround**: CNE upgrade should be performed during the maintenance window to minimize the impact.	2	24.1.1
37090973	NRF Access Token providing Access Token for NFType based even target plmn is not matching with NRF PLMN	When the access token request is initiated for an NF type, NRF doesn't validate if the *targetPlmn* matches with the NRF PLMN or not. It issues the token without validating the requester PLMN.	NRF will issue access token without validating the Requester PLMN. **Workaround**: There is no workaround available.	3	24.2.0

Note

Known bugs from 24.1.x and 24.2.x have been forward ported to Release 24.3.0.

4.3.6 NSSF Known Bugs

Release 24.3.2

There are no new known bugs in this release.

Release 24.3.1

There are no new known bugs in this release.

Release 24.3.0

Table 4-33 NSSF 24.3.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37048499	CNDB replication breaks post rollback to 24.2.1	CNDB uses binlogs for instruction replication across GR sites. High transaction rollbacks can degrade replication performance, leading to transaction order inconsistencies or constraint failures. NSSF's NsAvailability function may experience a replication break during rollback from version 24.2.x to 24.3.x if a delete and update occur close together.	Potential NsAvailability replication channel break during rollback. **Workaround**: Follow the replication recovery procedure in section 7.4.7.1 of the *Oracle Comminications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*.	2	24.3.0

Table 4-33 (Cont.) NSSF 24.3.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37136539	[dnsSrvEnabled: false] [peer health monitoring: disabled] NSSF not sending notification to peer2 if peer1 is down	With DnsServices disabled and static routes, notifications do not reroute when the primary peer is down.	Loss of notification in cases with static routing is witnessed. **Workaround**: Enable dnsSrv and use virtual FQDNs.	3	24.2.1
37099843	Upgrade 3 Site GR Setup, while upgrading NSSF and CNDB, we observed that the Ns-availability success rate dropped 0.07%, 0.77%, and 1.19%, respectively, for each site, and we got 500, 503, and 403, 408 error codes.	During an in-service upgrade, Ns-availability success rate drops slightly, with 500, 503, 403, and 408 errors at each site.	~0.25-1% of messages lost during upgrades. Impact is low; normal operation resumes post-upgrade. **Workaround**: There is no workaround available.	3	24.3.0
37136248	If dnsSrvEnabled is set to false and peer1 is used as a virtual host, the egress gateway will not sending the notifcation to peer2 host and peer health status is empty	With DnsServices disabled and static routes, notifications do not reroute when the primary peer is down.	Loss of notification in cases with static routing is witnessed. **Workaround**: Enable dnsSrv and use virtual FQDNs.	3	24.2.1

Table 4-33 (Cont.) NSSF 24.3.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37092299	NSSF 24.1.0 AMF Update procedure on Nnssf_NSSAIAvailability fails	Large availability updates take longer to respond, causing Ingress Gateway timeouts.	There is impact on NsAvailability traffic. **Workaround**: Increase timeout to 20 seconds in custom values.		
36889943	traffic moves from site2 to site1 , we are getting 404 error code for ns-availability scenarios	During site transitions, some NsAvailability PATCH messages receive 404 errors.	There is minor impact during handovers when PATCH occurs concurrently. **Workaround**: There is no workaround available.	3	24.2.0
36844482	Alternate-route cache not deleting SCP entry after TTL expiry	Alternate route service fails to delete entries after TTL expiry.	There is minor impact. **Workaround**: There is no workaround available.	3	24.2.0

Table 4-33 (Cont.) NSSF 24.3.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36734417	NSSF 2 Site GR :IN service solution Upgrade : 1.25K TPS : traffic loss of 0.259% and 0.027% at Site 1 and Site 2 during the NSSF upgrades, with latency of roughly 1.43 seconds and 886 ms.	~0.25% of messages experience latency or error responses during upgrade.	There is minor impact during upgrades with ~0.25% message loss. **Workaround**: There is no workaround available.	3	24.2.0
36552026	KeyId, certName, kSecretName, and certAlgorithm invalid values are not validating in the oauthvalidator configuration.	Validation is missing for KeyId, certName, kSecretName, and certAlgorithm fields in oauthvalidator.	There is no impact on traffic. **Workaround**: Use correct values during oauthvalidator configuration.	3	24.1.0
36285762	After restarting the NSselection pod, NSSF is transmitting an inaccurate NF Level value to ZERO percentage.	Inaccurate NF level value is transmitted by NSSF after NSselection pod restart.	There is no impact on traffic. **Workaround**: There is no workaround available.	3	23.4.0
36265745	NSSF is only sending NF-Instanse/NF-Service load level information for multiple AMF Get Requests	When multiple AMF requests are initiated to NsSelection, only some requests include NF-Instance or NF-Service LCI headers.	There is no impact on traffic. **Workaround**: There is no workaround available.	3	23.4.0

Table 4-33 (Cont.) NSSF 24.3.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35921656	NSSF should validate integer pod protection parameter limit	Missing validation in REST API for pod protection parameter.	Pod protection configuration is accepting invalid values. **Workaround**: Configure values according to guide recommendations.	3	23.3.0
35860137	In Policy Mapping Configuration in Ingress Gateway, For the samplingPeriod parameter, max value of parameter validation should be necessary.	There is missing validation for samplingPeriodparameter in Ingress Gateway Policy Mapping configuration.	There is no impact on traffic **Workaround**: Ensure correct values according to guide.	3	23.3.0
35922130	Key Validation is missing for IGW pod protection parameter name configuration	There is missing validation for pod protection parameter name in Ingress Gateway API configuration.	There is no impact on traffic **Workaround**: Follow the steps to configure proper values.	3	23.3.0
35888411	Wrong peer health status is coming "DNS SRV Based Selection of SCP in NSSF"	NSSF shows a non-existent SCP as healthy in cases of incorrect peer configuration.	There is no impact on traffic and no status is displayed for non-responsive SCPs. **Workaround**: There is no workaround available.		

Table 4-33 (Cont.) NSSF 24.3.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36881883	In Grafana, Service Status Panel is showing more than 100% for Ns-Selection and Ns-Avaliability Data	Grafana dashboard displays success rates exceeding 100%, which is incorrect.	There is no impact on traffic. **Workaround**: There is no workaround available.	4	24.2.0
36976984	["AutoConfigurationFromNsAvailability":"Disable"] When slice is allowed and AMF sends 2 times ns-avail add patch request, then NSSF should send a 400 error response appropriately explaining the failure reason and title for 2nd patch request	NSSF should return a 400 error for redundant add patch requests on restricted SNSSAI.	There is no impact as SNSSAI was already added in the initial request. **Workaround**: There is no workaround available.	4	24.2.0
36653494	If KID is missing in access token, NSSF should not send "Kid missing" instead of "kid configured does not match with the one present in the token"	NSSF should display "Kid missing" error rather than "kid configured does not match with the one present in the token".	There is no impact. **Workaround**: There is no workaround available.	4	24.1.0

Table 4-33 (Cont.) NSSF 24.3.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35855377	The abatementValue less than onsetValue should be validated by NSSF in the Overload Level Threshold Configuration.	There is missing validation for abatementValue less than onsetValue in overload configuration.	There is no impact. **Workaround**: Refer to Oracle Communications Cloud Native Core, Network Slice Selection Function Installation, Upgrade, and Fault Recovery Guide for correct values.	4	23.3.0
37023066	Delay of around 5 minutes observed for nrf-client-nfdiscovery to start during upgrade of NSSF	~5-minute delay for NRF client service startup during Helm install with ASM.	There is no impact. **Workaround**: There is no workaround available.		
35986361	NSSF will not modify the weight values in metrics simultaneously if the weight value changes. The weight metric has changed when any pod raises a new alarm.	NSSF alerts for pod protection only update when the state changes, not immediately after alert condition clears.	There is no impact. **Workaround**: There is no workaround available.	4	23.3.0

4.3.7 Policy Known Bugs

Table 4-34   Policy 24.3.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36832070	Issue with "Enforcement Network Element Name" blockly	The Policy Rule Engine (PRE) stops policy evaluation due to "Enforcement Network Element Name" blockly.	There is no signaling failure but some of the sessions are randomly responding with success without the charging rule. **Workaround**: There is no workaround available.	2	23.2.8
36913031	pcrf-core calls latency increases in seconds when bulwark locking mechanism is integrated with the Gx interface	PCRF Core call flow latency increases when Bulwark locking mechanism is integrated with the Gx interface.	PCRF Core call flow latency increases with bulwark integration. **Workaround**: There is no workaround available.	2	24.2.0
37246679	In case cm-service pod handling policy configuration import restarted, import stuck and subsequent import failed permanently	When the CM Service pod handling the import function restarts, the import gets stuck and subsequent import fails permanently.	If the previous import was interrupted due to pod restart, the subsequent import will fail until the database is cleaned up manually. **Workaround**: In the "importexportstatus" table in the CM Service, database has to be manually cleaned up by deleting the stale import status entry.	2	24.3.0

Table 4-34 (Cont.) Policy 24.3.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37234672	SMPCF: SQLException on put	The subscriber data is appended in large amount of Rx session information without any cleanup. Hence, the entries are reaching maximum allowed size and thus failing the PUT requests.	The "appSessionInfo" metadata is leaked in the SmPolicyAssociation and it increases the size of the session and eventually it increases to a level where it cannot be saved in the database. **Workaround**: Increase the concurrency lease duration time for the update notify messages towards SMF.	2	23.4.5
37203247	For DATA_Call performance observing high PDS latency when testing 15 KTPS each site (2-Site GR Setup)	In data call model performance run on a two-site georedundant setup, high PDS latency is observed when testing for 15K TPS traffic on each site.	Traffic is not sustaining at 15 KTPS on Site-2, and it drops significantly (< 10 KTPS). **Workaround**: There is no workaround available.	2	24.3.0
37202126	AM_UE Performance Continues ERROR "JDBC method pdssubscriber query on table saveSubscribers call failed and throw exception Row was updated or deleted by"was prompting in policyds while add some Burst or restarting Egress pods	During execution of 75K TPS traffic over AM and UE call performance run, if either by adding traffic burst or restarting Egress Gateway, PCF is throwing an error.	In execution of 75K TPS over AM and UE performance run, the test scenario of adding 8K traffic burst beyond the 100% of system capacity of 75K TPS throws error. This is still being investigated to find the exact root cause and impact, and whether congestion/overload control feature can fix this issue. **Workaround**: There is no workaround available.	2	24.3.0

Table 4-34 (Cont.) Policy 24.3.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37116139	Ingress Gateway configuration map lacks a listening path for UE Transfer Failure notifications on the Namf-comm interface	In the Ingress Gateway configuration map, the listening path for UE transfer failure notifications on the Namf Communication interface is missing.	The N1N2 transfer failure Notify Messages will not be processed by PCF UE service. As a result, any re-transmit configuration done for N1N2 transfer messages on failure will not take affect. This will cause T3501 timer expiry and the corresponding configuration will apply. **Workaround**: Add an additional path for transfer failure in the Ingress Gateway's configuration map.	3	24.3.0
37070113	SM Performance - Rolling back PCF from 23.4.6 to 23.4.4 nrf-dscovery pods stuck in crashloopback state	When rolling back PCF from 23.4.6 to 23.4.4, occasionally nrf-dscovery pod is stuck in crashloopback state.	In case the post-hook does not get executed for any reasons, two entries (one for release X and one for Y) can be seen in the database. NRF Managment pods remains in crashloopback state post rollback if a Method of Procedure (MOP) to remove the duplicate entries from the common config DB is not executed post rollback. **Workaround**: Customers already have a MOP to remove the duplicate entries from the common config DB post rollback.	2	23.4.6
36988075	After PCF pod restart one by one, occasionally we observed PCF performing duplicate subscription on NRF for peer NF	After all the PCF pods restart, occasionally it is observed that PCF is performing duplicate subscription on NRF for peer NF.	Due to duplicate subscription and multiple notifications received from NRF, the PCF won't be able to handle the NF profile updates. **Workaround**: Enable duplicate subscription feature on NRF if customer is using NRF.	2	24.2.0

Table 4-34 (Cont.) Policy 24.3.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36740591	PCF is not retrying PATCH with Updated ETAG if UDR respond with 412 Pre-Condition Failed	When UDR responds with "412 Precondition Failed" status code, PCF is not retrying PATCH request with updated Entity Tag (ETag).	The reported quota volume consumed in the CCR-T message for a specific scenario will not be updated on the UDR and thereby it will be lost. **Workaround**: There is no workaround available.	3	24.2.0
36915221	AM_UE Performance upgrade fails from PCF 24.1.0_GA to 24.2.0_rc7 " Error creating bean with name 'hookService' defined in URL"	Upgrade from any of the previous releases to Policy 24.2.0 fails due to Helm upgrade failure during post-upgrade job for Nrf-client-nfdiscovery. The Helm upgrade failure is due to an exception when deleting the older release entry from "common_configuration" table for Nrf-client-nfdiscovery service.	This upgrade failure causes traffic loss. **Workaround**: In case the upgrade from any of the previous releases to Policy 24.2.0 fails, retry the upgrade, which will delete the older version's configuration enabling upgrade to go through. If the retry fails, manually delete the older version entries from "common_configuration" table and retry the upgrade. This can bring up the services with latest versions configuration data.	3	24.2.0
37031750	On failures from BSF for pcfBinding delete, PCF not cleaning up contextBinding session on all N7/Rx session clean-up	PCF is not cleaning up contextBinding session on all N7/Rx session clean-up on failures from BSF for pcfBinding delete.	In case the BSF delete fails, the record will remain in the DB till the audit runs. **Workaround**: There is no workaround available.	3	24.2.0

Table 4-34 (Cont.) Policy 24.3.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37013029	PCF 23.4.3 (OCCNE 23.4.4) : Missing logs due to "Rejected by OpenSearch" error	OpenSearch is not be able to show the logs resulting in parsing error when Buffer Overflow error occurs.	OpenSearch will not be able to show the logs resulting in parse errorwhen Buffer Overflow error occurs. **Workaround**: There is no workaround available.	3	23.4.3
36944237	Blockly "Reported UsageData Limits" does not return DLP Name when DLP is created in CnPOLICY with just Name & MonKey	Currently, when the Data Limit profile name and limit ID are not the same, the desired policy does not work, and the top-up plan does not get activated.	Currently, when the data limit profile name and limit ID are not the same, the desired policy does not work, and the top-up plan does not get activated. It can be handled, and top-up can be activated. When the plan is provisioned in UDR, the mentioned policy works as expected. **Workaround**: Data Limit profile name and limitId should be the same in the Data Limit profile configuration in cn-policy.	3	24.2.0

> **Note**
>
> Known bugs from 24.1.0, 24.2.1, and 24.2.2 have been forward ported to Release 24.3.0.

4.3.8 OCCM Known Bugs

OCCM 24.3.0 Known Bugs

There are no known bugs in this release.

4.3.9 OCI Adaptor Known Bugs

OCI Adaptor 24.3.0 Known Bugs

There are no known bugs in this release.

4.3.10 SCP Known Bugs

Table 4-35 SCP 24.3.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37200182	Pod Overload control based on pending transactions has gauge metric ocscp_worker_pending_upstream_resp_count left with stale count	The pod overload control based on the pending transactions has gauge metric ocscp_worker_pending_upstream_resp_count left with stale count.	ocscp_worker_pending_upstream_resp_count might be observed with some stale count. **Workaround**: Perform either of the following actions:Disable the action for pending transaction overload configuration if it impacts performance. Restart the SCP-Worker pod to clear the stale count..	3	24.2.0

4.3.11 SEPP Known Bugs

SEPP 24.3.2

There are no known bugs in this release.

SEPP 24.3.1

There are no known bugs in this release.

Table 4-36 SEPP 24.3.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
36967443	N32 EGW Restart noticed on SEPP Site-1 & 2 after 48 hours of call-model run having MessageCopy Enabled	N32 Egress Gateway restarts on SEPP Site-1 and Site-2 after 48 hours of running the call model with MessageCopy enabled at both the PLMN-IGW and N32-EGW of the SEPP sites.	There is a traffic disruption during the restart. **Workaround**: There is no workaround available.	3	24.2.0
37213547	SEPP SCM CAT 0 not working for nsmf-pdusession release when body content is empty.	When a request is sent without a body, the Cat-0 screening works correctly. However, if the request has an empty body, it passes through screening incorrectly. The body needs to be screened for security reasons.	An empty body will get through the Cat-0 security feature. **Workaround**: There is no workaround available.	3	24.2.0
35898970	DNS SRV Support- The time taken for cache update is not same TTL value defined in SRV record.	The time it takes to update the cache doesn't match the time to live (TTL) value set in the SRV records. Sometimes the cache gets updated before the TTL expires, and other times it is updated after the TTL has passed. Expectation: The cache should be updated exactly according to the TTL. For example, if the TTL is set to 60 seconds, the cache should update 60 seconds after the TTL expires.	If the priority or weight is changed, it might take longer than the TTL for the cache to update and reflect those changes in the environment. **Workaround**: After changing the configuration, restart the n32-egress-gateway and the alternate-route service.	3	23.4.0

Table 4-36 (Cont.) SEPP 24.3.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
35919133	DNS SRV Support- Custom values key "dnsSrvEnabled" does not function as decsribed	The description for the custom values key dnsSrvEnabled states that it is a flag used to control whether DNS-SRV queries are sent to CoreDNS or not. If the flag is set to true, the request should go to CoreDNS. If the flag is set to false, the request should not be sent to CoreDNS. However, even when the flag is set to false and the setup is upgraded, the curl request still reaches CoreDNS. Scenario: The flag was set to false, and a peer configuration was created for the Virtual FQDN. The expectation was that, when executing the curl command, it is able to resolve the Virtual FQDN since the flag is false. Therefore, the request should not reach CoreDNS. However, this is not the case.	In the case of a virtual FQDN, the query will always be sent to CoreDNS. **Workaround**: Do not configure any records in CoreDNS.	3	23.4.0
36263009	PerfInfo calculating ambiguous values for CPU usage when multiple services mapped to single pod	In the cgroup.json file, multiple services are mapped to a single endpoint, making the calculation of CPU usage unclear. This is affecting the overall load calculation.	The overall load calculation is incorrect. **Workaround**: There is no workaround available.	3	23.4.1

Table 4-36 (Cont.) SEPP 24.3.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
36672487	No error thrown while enabling Discard Policy Mapping to true when corresponding discard policy is deleted	No error is thrown when enabling the Discard Policy Mapping to true, even if the corresponding discard policy has been deleted.	If the user enables the Discard Policy Mapping to true while the corresponding Discard Policy does not exist, no error will be displayed. **Workaround**: Helm configuration can be used to configure overload discard policies.	3	24.2.0
36605744	Generic error is thrown when wrong configuration is saved via GW REST APIs	A generic error ("Could not validate JSON") is thrown when incorrect configuration is saved via the Gateway REST APIs or CNC Console screen. The error message should specify which mandatory parameter is missing instead of being generic.	A generic error message makes it difficult for the user to troubleshoot the issue effectively. **Workaround**: There is no workaround available.	3	24.2.0
36614527	[SEPP-APIGW] Overload Control discard policies not working with REST API and CNCC	It is not possible to edit or change the default values of Overload Control discard policies. An error message stating "ocpolicymapping does not contain this policy name" appears when trying to save the configuration. The same behavior is observed when using the REST API.	The user will not be able to edit Overload Control discard policies through the CNC Console. **Workaround**: Helm configuration can be used to configure overload discard policies.	3	24.2.0

Table 4-36 (Cont.) SEPP 24.3.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release

36605719	Warnings being displayed while installing mediation due to k8sResource.container.prefix/suffix parameter	The warnings above are being displayed because the parameters `suffix` and `prefix` in the mediation charts have the value "{}".
		While the installation completes successfully, these warnings should not be displayed.
		`helm install -f custom.yaml ocsepp ocsepp/ -nns`
		`coalesce.go:286: warning: cannot overwrite table with non table for ocsepp.k8sResource.container.prefix (map[])`
		`coalesce.go:286: warning: cannot overwrite table with non table for ocsepp.k8sResource.container.suffix (map[])`
		`coalesce.go:286: warning: cannot overwrite table with non table for ocsepp.nf-mediation.global.k8sResource.container.prefix (map[])`
		`coalesce.go:286: warning: cannot overwrite table with non table for ocsepp.nf-mediation.global.k8sResource.container.suffix (map[])`
			Some warnings are displayed during the Helm installation.
			Workaround:
			There is no workaround available.
				4	24.1.0

Table 4-36 (Cont.) SEPP 24.3.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
36577846	improper value of InstanceIdentifier in oc_egressgateway_outgoing_tls_connections metric	The InstanceIdentifier in the oc_egressgateway_outgoing_tls_connections metric has an incorrect value.	The InstanceIdentifier value will be incorrect in the TLS connection metrics, but the metrics can still be uniquely identified by the namespace name. **Workaround**: There is no workaround available.	4	24.1.0
37128268	Error in request not shown in Jaeger	Requests are received from PLMNs that aren't available in the Remote SEPP. The incoming trace appears in Jaeger, but the error response sent to the producer isn't shown.	Error responses are not tracked using Jaeger. **Workaround**: There is no workaround available.	4	24.1.0

4.3.12 UDR Known Bugs

Table 4-37 UDR 24.3.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36381825	Helm chart does not pass Helm Strict Linting	Helm chart is not passing Helm strict linting.	The duplicate errors from Helm strict lint must be ignored. **Workaround**: There is no workaround available.	3	22.3.2

4.3.13 Common Services Known Bugs

4.3.13.1 ATS Known Bugs

ATS 24.3.0 Known Bugs

There are no known bugs in this release.

4.3.13.2 ASM Configuration Known Bugs

Release 24.3.0

There are no known bugs in this release.

4.3.13.3 Alternate Route Service Known Bugs

Table 4-38 Alternate Route Service 24.3.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36935315	Implement SA Guidelines for SecurityContext Configuration on GW	Gateway Services implemented security context at container level with a control parameter that can enable and disable the security context from the values.yaml file. However, a few more parameters are required to be added to the security context to achieve these requirements from other NFs.	These changes are required for security checks, and the additional parameters requested will have enhanced security, however, the absence of these parameters will not impact existing applications. **Workaround**: There is no workaround available.	3	24.3.0

4.3.13.4 Egress Gateway Known Bugs

Table 4-39 Egress Gateway 24.3.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36935315	Implement SA Guidelines for SecurityContext Configuration on GW	As per the Gateway Services 24.3.0, SecurityContext configuration was added to Gateway Services Helm charts. However, Gateway Services support allowPrivilegeEscalation, dropAllCapabilities, and addCapabilities.	These changes are required for security checks, and the additional parameters requested will have enhanced security, however, the absence of these parameters will not impact existing applications. **Workaround**: There is no workaround available.	3	23.4.0
36928822	No error codes observed in the Egress GW Grafana dashboard when FQDN is mis-configured	After providing 1% traffic on the new site 002, 500 internal errors occurred in the egress-gw pod logs becasue SCP FQDN was not configured properly. No error codes are observed on the Egress Gateway Grafana dashboard.	Metric is not getting pegged when incorrect virtual host is configured in Egress Gateway. **Workaround**: There is no workaround available.	3	23.4.4

Table 4-39 (Cont.) Egress Gateway 24.3.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35948415	The PUT API allows you to add cause values to the "sbiroutingerrorcriteriasets" in policy 23.2.2.	The PUT API allows you to add cause values to sbiroutingerrorcriteriasets in Policy 23.2.2. The following parameters are introduced in the Error cause-based re-try feature in 23.2.6 and 23.4.0 patch releases, however, these parameters could be configured in the previous releases: "cause": { "path": ".cause", "reason": ["UNSPECIFIED_MSG_FAILURE", "SUBSCRIPTION_NOT_FOUND"],	Non-applicable configuration is being allowed with PUT API operation. **Workaround**: There is no workaround available.	3	23.2.2
36730017	Register request towards alternate-route is giving incorrect response of 200	While performing the register request, Gateway Services received a 200 OK response, where the FQDN entry is not present in the DNS server.	While performing Alternate Route Services register request, success response is received when the FQDN entry is absent in the DNS server. **Workaround**: There is no workaround available.	4	24.1.0

4.3.13.5 Ingress Gateway Known Bugs

Table 4-40 Ingress Gateway 24.3.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37172147	IGW pods restarting continuously with exit code 127 and 137 around 6K traffic (AM create and delete)	Ingress Gateway pods are continuously restarting for 10 minutes and becoming stable after some time.	An unstable or slow remote peer or abrupt deletion of a remote peer of an Ingress Gateway can cause overload at Gateway Services pods. **Workaround**: To protect Gateway Services pods, the existing Ingress Gateway Pod Protection feature shall be enabled at Gateway Services.	2	24.3.1

Table 4-40 (Cont.) Ingress Gateway 24.3.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37134318	CNE Upgrade : Traffic loss from IGW to discovery	There is a loss of traffic from Ingress Gateway to Discovery while performing the CNE upgrade process only in case of a non ASM setup.	Loss of traffic is observed at Ingress Gateway when NF back-end microservices are removed from the worker node that is going into the maintenance mode. **Workaround**: The DNS Refresh Scheduler timer can be set to a lower value. Low number of pods are deleted when worker node is put into maintenance. Spread the downtime across all worker nodes.	2	24.1.0
36935315	Implement SA Guidelines for SecurityContext Configuration on GW	Gateway Services implemented security context at container level with a control parameter that can enable and disable the security context from the values.yaml file. However, a few more parameters are required to be added to the security context to achieve these requirements from other NFs.	These changes are required for security checks, and the additional parameters requested will have enhanced security, however, the absence of these parameters will not impact existing applications. **Workaround**: There is no workaround available.	3	24.3.0

Table 4-40 (Cont.) Ingress Gateway 24.3.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35983677	NRF- Missing mandatory "iat claim" parameter validation is not happening in CCA header for feature - CCA Header Validation	As per the feature description, "iat" is a mandatory parameter in JWT claims. When CCA header request is sent without "iat" claim and "maxTokenAge": 0 is set in /nrf/nf-common-component/v1/igw/ccaheader. The missing mandatory parameter is not validated, and the CCA header request gets accepted by NRF.	Mandatory validation to be performed on parameter would be missed at Gateway Services and request would be processed. **Workaround**: There is no workaround available.	3	23.2.0
36464641	When feature Ingress Gateway POD Protection disabled at run time alerts are not getting cleared and metrics are getting pegged in NRF 23.4.0	When the Ingress Gateway Pod Protection feature is disabled at run time, alerts are not getting cleared and metrics are getting pegged in NRF 23.4.0.	Alerts are not getting cleared and metrics would be pegged even when feature is disabled during run time. **Workaround**: There is no workaround available.	3	23.4.0

Table 4-40   (Cont.) Ingress Gateway 24.3.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35526243	Operational State change should be disallowed if the required pre-configurations are not present	Currently, the operational state at Ingress Gateway can be changed even if thecontrolledshutdownerrormapping and errorcodeprofiles are not present. Thisindicates that the required action of rejecting traffic will not occur. There must be a pre-check to check for these configurations before allowingthe state to be changed. If the pre-check fails, the operational state shouldnot be changed.	Request will be processed by Gateway Services when it is supposed to be rejected. **Workaround**: There is no workaround available.	3	23.2.0
34610831	IGW is accepting incorrect API names with out throwing any error	Ingress Gateway is accepting incorrect API names without displaying any error. If there is a typo in the configuration UDR, the command should get rejected. Otherwise, it gives the wrong impression that the configuration is correct but the desired behavior is not observed.	The non-existing resource name would be pretended to be successfully updated in REST configurations. **Workaround**: There is no workaround available.	3	22.2.4

Table 4-40 (Cont.) Ingress Gateway 24.3.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35913189	Missing validation of the failureReqCountErrorCodeSeriesId mandatory parameter in the Ingress Gateway's Routes Configuration	As per NSSF_REST_Specification_Guide, Section 5.2.1.5, failureReqCountErrorCodeSeriesId is a mandatory parameter for Routes Configuration in Ingress Gateway. The request is rejected by Ingress Gateway when the failureReqCountErrorCodeSeriesId parameter is not present in the JSON payload.	Requests will be processed by considering the mandatory configuration from the existing deployment configuration when it is not configured through REST APIs. **Workaround**: There is no workaround available.	4	23.3.0

4.3.13.6 Common Configuration Service Known Bugs

Common Configuration Service 24.3.0 Known Bugs

There are no known bugs in this release.

4.3.13.7 Helm Test Known Bugs

Release 24.3.0

There are no known bugs in this release.

4.3.13.8 NRF-Client Known Bugs

Table 4-41 NRF-Client 24.3.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37010007	After PCF pod restart, occasionally we observed PCF performing duplicate subscription on NRF for peer NF.	After PCF pod restart, PCF is performing duplicate subscription on NRF for peer NF.	During NRF-Client management pod initialization, NRF-Client will end up in creating a duplicate subscription in NRF, if the config-server throws error while NRF-client checking for existing subscriptions in the DB. These duplication subscription will result into NRF-Client processing duplicate notifications. **Workaround**: To avoid duplicate subscription/	2	24.2.0

Table 4-41 (Cont.) NRF-Client 24.3.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
			Notification, allowDuplicateSubscription can be set to false in NRF, by which NRF will not create duplicate subscription, hence reducing duplicate Notification as well.		

4.3.13.9 App-Info Known Bugs

Release 24.3.0

There are no known bugs in this release.

4.3.13.10 Perf-Info Known Bugs

Perf-Info 24.3.0 Known Bugs

There are no known bugs in this release.

4.3.13.11 Debug Tool Known Bugs

Release 24.3.0

There are no known bugs in this release.