Oracle® Communications

Cloud Native Core Release Notes

Release 3.24.1
F96345-18
December 2024

Oracle Communications Cloud Native Core Release Notes, Release 3.24.1

F96345-18

Contents

4 Resolved and Known Bugs

My Oracle Support

My Oracle Support (https://support.oracle.com) is your initial point of contact for all product support and training needs. A representative at Customer Access Support can assist you with My Oracle Support registration.

Call the Customer Access Support main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. When calling, make the selections in the sequence shown below on the Support telephone menu:

- For Technical issues such as creating a new Service Request (SR), select **1**.
- For Non-technical issues such as registration or assistance with My Oracle Support, select **2**.
- For Hardware, Networking and Solaris Operating System Support, select **3**.

You are connected to a live agent who can assist you with My Oracle Support registration and opening a support ticket.

My Oracle Support is available 24 hours a day, 7 days a week, 365 days a year.

What's New In This Guide

Release 3.24.1 - F96345-18, December 2024

CNC Console 24.1.1 Release

Updated the following sections with the details of CNC Console release 24.1.1:

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

cnDBTier 24.1.2 Release

Updated the following sections with the details of cnDBTier release 24.1.2:

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

Release 3.24.1 - F96345-17, October 2024

cnDBTier 24.1.2 Release

Updated the following sections with the details of cnDBTier release 24.1.2:

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

Release 3.24.1 - F96345-16, October 2024

CNE 24.1.2 Release

Updated the following sections with the details of CNE release 24.1.2:

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

Release 3.24.1 - F96345-15, October 2024

SCP 24.1.2 Release

Updated the following sections with the details of SCP release 24.1.2:

- Media Pack

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

Release 3.24.1 - F96345-14, September 2024

NRF 24.1.3 Release

Updated the following sections with the details of NRF release 24.1.3:

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

NRF 24.1.2 Release

Updated the following sections with the details of NRF release 24.1.2:

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

Release 3.24.1 - F96345-12, July 2024

UDR 24.1.1 Release

Updated the following sections with the details of UDR release 24.1.1:

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

Release 3.24.1 - F96345-11, July 2024

Made formatting changes.

Release 3.24.1 - F96345-10, July 2024

CNE 24.1.1 Release

Updated the following sections with the details of CNE release 24.1.1:

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

Release 3.24.1 - F96345-09, July 2024

cnDBTier 24.1.1 Release

Updated the following sections with the details of cnDBTier release 24.1.1:

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

Release 3.24.1 - F96345-08, July 2024

Policy 24.1.0 Release

Updated the Compatibility Matrix section for Policy 24.1.0.

BSF 24.1.0 Release

Updated the Compatibility Matrix section for BSF 24.1.0.

Release 3.24.1 - F96345-07, July 2024

Policy 24.1.0 Release

Updated the Compatibility Matrix section with supported CNE and Kubernetes versions for Policy 24.1.0.

BSF 24.1.0 Release

Updated the Compatibility Matrix section with supported CNE and Kubernetes versions for BSF 24.1.0.

Release 3.24.1 - F96345-06, June 2024

SCP 24.1.0 Release

Updated the SCP Resolved Bugs section with a new bug for SCP-ATS release 24.1.1.

Release 3.24.1 - F96345-05, June 2024

NSSF 24.1.1 Release

Updated the following sections with the details of NSSF release 24.1.1:

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

- NSSF Resolved Bugs

Release 3.24.1 - F96345-04, June 2024

NRF 24.1.1 Release

Updated the following sections with the details of NRF release 24.1.1:

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

Release 3.24.1 - F96345-03, May 2024

Updated the known bugs for 24.1.0 in the cnDBTier Known Bugs section.

Release 3.24.1 - F96345-02, April 2024

BSF 24.1.0 Release

Updated the following sections with the details of BSF release 24.1.0:

- 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

CNE 24.1.0 Release

Updated the following sections with the details of CNE release 24.1.0:

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

OSO 24.1.0 Release

Updated the following sections with the details of OSO release 24.1.0:

- OSO
- Media Pack
- Compatibility Matrix

NSSF 24.1.0 Release

Updated the following sections with the details of NSSF release 24.1.0:

- 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

Policy 24.1.0 Release

Updated the following sections with the details of Policy release 24.1.0:

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

SCP 24.1.0 Release

Updated the following sections with the details of SCP release 24.1.0:

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

Release 3.24.1 - F96345-01, April 2024

ATS 24.1.0 Release

Updated the following sections with the details of ATS release 24.1.0:

- Automated Testing Suite (ATS) Framework
- ATS Resolved Bugs
- ATS Known Bugs

CNC Console 24.1.0 Release

Updated the following sections with the details of CNC Console release 24.1.0:

- Cloud Native Configuration Console (CNC Console)
- Media Pack
- Compatibility Matrix
- 3GPP Compatibility Matrix
- Common Microservices Load Lineup
- Security Certification Declaration
- CNC Console Resolved Bugs

cnDBTier 24.1.0 Release

Updated the following sections with the details of cnDBTier release 24.1.0:

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

NEF 24.1.0 Release

Updated the following sections with the details of NEF release 24.1.0:

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

NRF 24.1.0 Release

Updated the following sections with the details of NRF release 24.1.0:

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

OCCM 24.1.0 Release

Updated the following sections with the details of OCCM release 24.1.0:

- Oracle Communications Cloud Native Core, Certificate Management (OCCM)
- Media Pack

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

OCI Adaptor 24.1.0 Release

Updated the following sections with the details of OCI Adaptor release 24.1.0:

- OCI Adaptor
- Media Pack
- Compatibility Matrix
- OCI Adaptor Known Issue

SEPP 24.1.0 Release

Updated the following sections with the details of SEPP release 24.1.0:

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

UDR 24.1.0 Release

Updated the following sections with the details of UDR release 24.1.0:

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

Common Services 24.1.0 Resolved Bugs

Updated the following sections with the details of Common Services 24.1.0 Resolved Bugs:

- Common Configuration Service Resolved Bugs
- Egress Gateway Resolved Bugs
- Ingress Gateway Resolved Bugs
- Alternate Route Service Resolved Bugs

1 Introduction

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

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

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

2
Feature Descriptions

This chapter provides a summary of new features and updates to the existing features for network functions released in Cloud Native Core release 3.24.1.

2.1 Automated Testing Suite (ATS) Framework

Release 24.1.0

Oracle Communications Cloud Native Core, Automated Test Suite (ATS) framework 24.1.0 has been updated with the following enhancements:

- **ATS GUI Enhancements**: With this enhancement, the ATS Graphical User Interface (GUI) layout is redesigned to streamline user interaction by segregating execution options and features or test cases into distinct compartments, allowing the users to navigate effortlessly between different functionalities. For more information, see the "*ATS GUI Enhancements*" section in *Oracle Communications Cloud Native Core, Automated Testing Suite Guide.*
- **Multiselection Capability for Features and Scenarios**: ATS allows users to select and run single or multiple features and scenarios by selecting a check box for the corresponding features or scenarios. For more information, see the "*Multiselection Capability for Features and Scenarios*" section in *Oracle Communications Cloud Native Core, Automated Testing Suite Guide.*
- **Support for ATS Deployment in OCI**: This feature allows users to deploy and run ATS in an Oracle Cloud Infrastructure (OCI) environment. For more information, see the "*Support for ATS Deployment in OCI*" section in *Oracle Communications Cloud Native Core, Automated Testing Suite Guide.*

2.2 Binding Support Function (BSF)

Release 24.1.0

Oracle Communications Cloud Native Core, Binding Support Function (BSF) 24.1.0 has been updated with the following enhancements:

- **Support for cnDBTier functionalities in CNC Console:** With this enhancement, cnDBTier functionalities are integrated into the CNC Console, and users can view specific cnDBTier statuses on the CNC Console. For more information, see "*Support for cnDBTier Functionalities in CNC Console*" in *Oracle Communications Cloud Native Core, Binding Support Function User Guide*.
- **Support for Automated PKI Integration**: BSF supports automation of certificate lifecycle management in integration with Oracle Communications Cloud Native Core Certificate Manager (OCCM). This allows to automatically create, renew, and delete certificates for a given CA, with the possibility to track previously created certificates and renew or delete them when required. For more information, see "*Support for Automated Certificate Lifecycle Management*" section in *Oracle Communications Cloud Native Core, Binding Support Function User Guide*.
- **Validating Destination Realm Received in AAR-I Message**: The Destination-Realm Attribute-Value Pair (AVP) received in the AAR-I message from an AF is validated at the

BSF Diameter Gateway before processing and forwarding the AAR-I message to a corresponding PCF instance. This validation applies exclusively to the AAR-I message within the BSF. For more information, see "*Validating Destination Realm Received in AAR-I Message*" section in *Oracle Communications Cloud Native Core, Binding Support Function User Guide.*

- **MultiSelection Capability for Features and Scenarios**: ATS allows users to select and run single or multiple features and scenarios by selecting a check box for the corresponding features or scenarios. For more information, see the "*Multiselection Capability for Features and Scenarios*" section in *Oracle Communications Cloud Native Core, Automated Testing Suite Guide*.
- **Individual Stage Group Selection**: This feature allows users to select and execute a single or multiple stages or groups by selecting a check box for the corresponding stage or group. For more information, see "*Individual Stage Group Selection*" section in *Oracle Communications Cloud Native Core, Automated Test Suite Guide*.

2.3 Cloud Native Core cnDBTier

Release 24.1.2

Oracle Communications Cloud Native Core, cnDBTier (cnDBTier) 24.1.2 has been updated with the following enhancements:

- **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*.

> **Note:**
>
> The recommended value of the `HeartbeatIntervalDbDb` parameter is updated to "1250" in this release. When you upgrade cnDBTier, check the value of `HeartbeatIntervalDbDb` in the running cnDBTier instance. If the value is not set to "1250", then update the value to "1250" step by step. For the steps to increase or decrease the `HeartbeatIntervalDbDb` value, see the "Upgrading cnDBTier Clusters" section in *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*.

Release 24.1.1

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

Release 24.1.0

Oracle Communications Cloud Native Core, cnDBTier (cnDBTier) 24.1.0 has been updated with the following enhancements:

- **TLS v1.3 Support for Georeplication**: With this feature, cnDBTier supports TLS 1.3 for georeplication. On enabling this feature, the replication SQL pod uses the certificates

provided or configured to establish an encrypted connection for georeplication. This ensures that the replication data transfer is secure. cnDBTier supports the creation of TLS 1.3 connections and mandatory ciphers and extensions. For more information about this feature, see *Oracle Communications Cloud Native Core, cnDBTier User Guide* and *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*.
Consideration: If you are enabling TLS for the replication channels, be informed that cnDBTier doesn't support addition and removal of replication channel groups on cnDBTier setups where TLS is enabled.

- **REST APIs to Display cnDBTier Health Status on CNC Console**: In this release, cnDBTier exposes the following REST APIs to CNC Console:
  - Health status of replication service
  - Health status of monitor service
  - Overall health status of NDB data service
  - Health status of backup manager service

  CNC Console uses these REST APIs to fetch cnDBTier health status data and display them on the CNC Console GUI. This way, cnDBTier facilitates users (NFs) to integrate and view the health status of cnDBTier services on CNC Console. For more information about this feature and the REST APIs, see *Oracle Communications Cloud Native Core, cnDBTier User Guide*.
- **Multithreaded Applier (MTA)**: The MTA feature provides the functionality to allow independent binlog transactions to be run in parallel at a replica thereby increasing the peak replication throughput. NDB replication is modified to support the use of generic MySQL server MTA mechanism. This feature was disabled until the previous release due to technical issues. cnDBTier 24.1.0 supports MTA feature by resolving the issues. For more information about this feature, see *Oracle Communications Cloud Native Core, cnDBTier User Guide* and *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*.
- **Support for New Versions of Software**: Oracle MySQL Cluster Database version has been updated to 8.0.36.

2.4 Cloud Native Configuration Console (CNC Console)

Release 24.1.1

There are no new features or enhancements in this release.

Release 24.1.0

Oracle Communications Cloud Native Configuration Console (CNC Console) 24.1.0 has been updated with the following enhancements:

- **Deployment in OCI using OCI Adaptor**: Oracle Cloud Infrastructure (OCI) is a set of complementary cloud services that enable you to build and run a range of applications and services in a High Availability (HA) hosted environment. CNC Console can be integrated into the OCI using the OCI Adaptor.
  OCI Adaptor provides a smooth integration to CNC Console observability and monitoring modules with OCI observability and management, enabling the users to have access of alerts, metrics, and KPIs on the OCI platform. For more information on deploying CNC Console in OCI, see *Oracle Communications Cloud Native Configuration Console User Guide* and *Oracle Communications Cloud Native Configuration Console Installation,*

Upgrade, and Fault Recovery Guide, and *Oracle Communications Cloud Native Core, OCI Adaptor Deployment Guide*.

- **CNC Console Integration with Network Exposure Function (NEF) (Excluding CAPIF Integration)**: The integration of NEF with the CNC Console enables you to configure and modify different services and features using the CNC Console. As a part of this feature, authentication and authorization of API and GUI requests, metrics, alerts, and KPIs are now supported. For more information, see *Oracle Communications Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide* and *Oracle Communications Cloud Native Configuration Console User Guide*.
- **NF Versions Supported by CNC Console**:
  - SCP 24.1.x
  - NRF 24.1.x
  - UDR 24.1.x
  - BSF 24.1.x
  - Policy 24.1.x
  - SEPP 24.1.x
  - NSSF 24.1.x
  - NEF 24.1.x
  - DD 24.1.x
  - NWDAF 24.1.x
  - OCCM 24.1.x

2.5 Cloud Native Environment (CNE)

Release 24.1.2

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

Release 24.1.1

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

Release 24.1.0

Oracle Communications Cloud Native Core, Cloud Native Environment (CNE) 24.1.0 has been updated with the following enhancements:

- **Support for externalTrafficPolicy**: With this release, CNE supports externalTrafficPolicy which is a Kubernetes feature. Starting this release, LoadBalancer services can add and set the `externalTrafficPolicy` attribute to `Local`. When this attribute is set, lb-controller directs the traffic to only the nodes where service endpoint pods are deployed. This change does not impact the original functionality. To use this feature, Network Functions (NFs) must deploy their services with the `externalTrafficPolicy` set to `Local`, and update their Helm charts and manifest file to include this attribute.
- **New Versions of Common Services**: The following common services are upgraded in this release:
  - Helm - 3.13.2
  - Kubernetes - 1.28.6

- containerd - 1.7.1
- Calico - 3.26.4
- MetalLB - 0.13.11
- Prometheus - 2.51.1
- Grafana - 9.5.3
- Jaeger - 1.52.0
- Istio - 1.18.2
- Kyverno - 1.9
- cert-manager - 1.12.4
- Prometheus Operator - 0.70.0

To get the complete list of third-party services and their versions, refer to the `dependencies_24.1.0.tgz` file provided as part of the software delivery package.

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.

OSO Release 24.1.0

Oracle Communications Operations Services Overlay 24.1.0 has been updated with the following enhancements:

Support for new versions:

- AlertManager version is uplifted from version from 0.26.1 to 0.27.0.
- nginx version is uplifted from version 1.9.4 to 1.10.0.
- Prometheus version is uplifted from version 2.44.0 to 2.50.1.

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

2.6 Network Exposure Function (NEF)

Release 24.1.0

Oracle Communications Cloud Native Core, Network Exposure Function (NEF) 24.1.0 has been updated with the following enhancements:

- **NEF Integration with the CNC Console**: The integration of NEF with the CNC Console enables you to configure and modify different services and features using the CNC Console. For more information, see "*Configuring Network Exposure Function using the CNC Console*" in *Oracle Communications Cloud Native Core, Network Exposure Function User Guide*.
- **Support for MSISDN-Less MO-SMS**: This feature enables NEF to deliver the MSISDN-less MO-SMS notification message from Short Message Service - Service Center (SMSSC) to Application Function (AF). It allows user equipment (UE) to send messages to AF without using Mobile Station International Subscriber Directory Number (MSISDN) through T4 interface. For more information, see "*Support for MSISDN-Less MO-SMS*" in *Oracle Communications Cloud Native Core, Network Exposure Function User Guide*.

2.7 Network Repository Function (NRF)

Release 24.1.3

There are no new features or enhancements in this release.

Release 24.1.2

There are no new features or enhancements in this release.

Release 24.1.1

Oracle Communications Cloud Native Core, Network Repository Functions (NRF) 24.1.1 has been updated with the following enhancement:
Support for NRF 76.4K TPS with Growth Feature: With this enhancement, NRF supports 76.4K TPS with NRF Growth feature enabled. For more information, see *Oracle Communications Cloud Native Core, Network Repository Function Benchmarking Guide.*

Release 24.1.0

Oracle Communications Cloud Native Core, Network Repository Functions (NRF) 24.1.0 has been updated with the following enhancements:

- **Support for cnDBTier Health APIs in CNC Console**: With this enhancement, cnDBTier health APIs are also integrated into the CNC Console, and users can view specific cnDBTier APIs on the CNC Console. For more information, see "*cnDBTier APIs*" in the *Oracle Communications Cloud Native Core, Network Repository Function User Guide*.
- **Error Response Enhancement in NRF**: This feature enhances the details attribute in the error response to more accurately identify source of error and cause of error. For more information, see "*Error Response Enhancement for NRF*" in the *Oracle Communications Cloud Native Core, Network Repository Function User Guide*.
- **SLF Lookup for PCF**: The Subscriber Location Function (SLF) feature of NRF is enhanced to support the discovery of Policy Control Function (PCF) when a Subscription Permanent Identifier (SUPI) or Generic Public Subscription Identifier (GPSI) subscriber identities are received in the discovery query. NRF then returns the matching PCFs based on the groupId to the requester NF. For more information about the "*Subscriber Location Function*" feature, see *Oracle Communications Cloud Native Core, Network Repository Function User Guide*.
- **Support for Service Level Priority with Same Service Names**: The Preferred Locality priority handling has been enhanced to support service level priority with the same service names. After processing a service-name based discovery query, the NRF updates the priority levels for both the profile and service within the NF profile if there are multiple services with the same name. For more information about the feature, see "*Preferred Locality*" in *Oracle Communications Cloud Native Core, Network Repository Function User Guide*.
- **Support for configuring Ingress Gateway and Egress Gateway APIs in CNC Console**: The configuration for Ingress Gateway and Egress Gateway APIs was earlier supported only using REST. With the implementation of this feature, NRF now supports the configuration of Ingress Gateway and Egress Gateway APIs using the CNC Console. For more information about the feature, see the "Configuring NRF using CNC Console" chapter in *Oracle Communication Cloud Native Core, Network Repository Function User Guide*.

- **Deployment in OCI using OCI Adaptor**: Oracle Cloud Infrastructure (OCI) is a set of complementary cloud services that enable you to build and run a range of applications and services in a High Availability (HA) hosted environment. NRF can be integrated into the OCI using the OCI Adaptor.
  OCI Adaptor provides a smooth integration to NRF observability and monitoring modules with OCI observability and management, enabling the users to have access of alerts, metrics, and KPIs on the OCI platform. For more information on deploying NRF in OCI, see *Oracle Communications Cloud Native Core, Network Repository Function User Guide* and *Oracle Communications Cloud Native Core, Network Repository Function Installation, Upgrade, and Fault Recovery Guide*, and *Oracle Communications Cloud Native Core, OCI Adaptor Deployment Guide*.

2.8 Network Slice Selection Function (NSSF)

Release 24.1.1

There are no updates to features in this release.

Release 24.1.0

Oracle Communications Cloud Native Core, Network Slice Selection Function (NSSF) 24.1.0 has been updated with the following enhancements:

- **Support for Common Service APIs in CNC Console**: The configuration for common service APIs was earlier supported only using REST. With the implementation of this feature, NSSF now supports the configuration of Ingress Gateway and Egress Gateway parameters using the CNC Console. You can perform HTTP methods such as GET and PUT using the CNC Console. For more information, see "*Support for Common Service APIs in CNC Console*" section in *Oracle Communications Cloud Native Core, Network Slice Selection Function User Guide*.
- **Support for cnDBTier Functionalities in CNC Console:** With this enhancement, cnDBTier functionalities are integrated into the CNC Console, and users can view specific cnDBTier statuses on the CNC Console. For more information, see "*Configuring NSSF using CNC Console*" section in *Oracle Communications Cloud Native Core, Network Slice Selection Function User Guide*.
- **Enhanced Computation of AllowedNSSAI in NSSF**: This feature provides NSSF the flexibility in NSSAI handling based on 3GPP specifications and subscriber details. When the feature is enabled, NSSF creates Allowed-NSSAI based on UE subscription details and Tracking Area support. When it is disabled, NSSF adheres to the 3GPP specification 29.531 for constructing AllowedNSSAI based on the intersection of Requested and Subscribed NSSAI, along with operator policy considerations. For more information, see "*Enhanced Computation of AllowedNSSAI in NSSF*" section in *Oracle Communications Cloud Native Core, Network slice Selection Function User Guide*.
- **Configuration of SNMP Notifier**: With this release, NSSF supports configuration of SNMP notifier using MIB files. The SNMP MIB files are used to define the MIB objects. When uploaded to Wireshark and MIB tools, such as MIB Browser and Trap Receiver, users can see the detailed MIB definition instead of just the OID. For more information, see "*Configuring SNMP Notifier*" section in *Oracle Communications Cloud Native Core, Network slice Selection Function User Guide*.

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

Release 24.1.0

Oracle Communications Cloud Native Core, Certificate Management (OCCM) 24.1.0 has been updated with the following enhancements:

- **HTTPs support for CA communication**: OCCM has now enabled HTTPs support for connections between OCCM and CA. With this feature, OCCM, as a client, will validate the certificate presented by CA during the TLS handshake. For more information, see *Oracle Communications Cloud Native Core, Certificate Management User Guide.*

2.10 OCI Adaptor

Release 24.1.0

Oracle Cloud Infrastructure (OCI) deployment, introduced in CNC 3.24.1, enables you to build and run a range of applications and services in a High Availability (HA) hosted environment. OCI Adaptor provides a smooth integration to the NF's observability and monitoring modules with OCI observability and management, enabling the users to have access of alerts, metrics, and KPIs on the OCI platform. OCI Adaptors are a combination of open source, OCI owned enablers and customized enablers that acts as a conduit between NFs and OCIs observability services.

The deployment of OCI-Adaptors includes Management-Agent, OTEL Collector, Metrics-Server, Scrape-Target-Discovery-Container and Fluentd.

- **Management Agent**: Management-Agent is a service that provides low latency interactive communication and data collection between Oracle Cloud Infrastructure and any other targets.
  As a part of OCI Adaptor, management agent is used to collect metrics data from multiple applications deployed on the OKE cluster and push them to OCI telemetry service.

  But Management-Agent cannot dynamically pull or stop pulling the metrics data from the new pods getting spanned in the cluster and old pods getting deleted. To overcome this limitation another application has been developed by the engineering called as **scrape-target-discovery** container.

  - **Scrape-Target-Discovery Container**:
    This container provides the following functionality:

    1. It discovers the PODs to be scraped (prior to scraping).
    2. It creates one config/properties file for each scrape target.
    3. It also purges the obsolete config files i.e. the scrape targets config files which are no longer active in the OKE cluster.

  - **Metrics Server**: Metric server is a part of management-agents helm charts and thus is deployed along with management-agent. This is used to collect the cAdvisor metrices and pass them to OCI monitoring service using management-agent.
- **Fluentd:**
  The OCI's customized Fluentd collects the log data from the various configured log sources and routes the collected log data over the Oracle cloud logging analytics service.

Since the microservices deployed in OKE K8 cluster stores the log data on the worker nodes, Fluentd is deployed as a daemonset to collect the log data from all the available worker nodes.

- **OTEL Collector:**
  CNC applications uses OpenTelemetry SDK and OTLP span exporter to generate and share the span data. OTEL collector is responsible for receiving, processing, and batching the span data to traces and eventually export the trace data over OCIs APM (Application Performance Monitoring) service.
- **NF Versions Supported by OCI Adaptor:**
  - CNC Console 24.1.0
  - OCNADD 24.1.0
  - SEPP 24.1.0
  - SCP 24.1.0
  - NRF 24.1.0

For more information on deploying the NFs on OCI, see the NF specific Installation, Upgrade, and Recovery Guide.

2.11 Policy

Release 24.1.0

Oracle Communications Cloud Native Core, Converged Policy 24.1.0 has been updated with the following enhancements:

- **Support for cnDBTier functionalities in CNC Console:** With this enhancement, cnDBTier functionalities are integrated into the CNC Console, and users can view specific cnDBTier statuses on the CNC Console. For more information, see "*Support for cnDBTier Functionalities in CNC Console*" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.
- **Enhancement to PRE Metrics:** With this enhancement, Policy blocks have been added to PRE to evaluate policy processing time, policy block execution counter, and policy blocks execution time. For more information about the blocks, see "*Public Category*" section in *Oracle Communications Cloud Native Core, Converged Policy Design Guide*. For more information about the feature, see "*Enhancement to PRE Metrics*" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.
- **Support for Handling Reduced Capability Devices**: Policy supports the handling of requests from reduced capability devices (RedCap) to support IoT ecosystem. Policy identifies the incoming request from the RedCap devices and interacts with PRE to make appropriate decisions for the reduced capability devices. Currently, this feature is implemented only for create, update, update notify, and delete call flows for SM service. For more information, see "*Support for Handling Reduced Capability Devices*" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.
- **Support for Automated PKI Integration**: Policy supports automation of certificate lifecycle management in integration with Oracle Communications Certificate Manager (OCCM). This allows to automatically create, renew, and delete certificates for a given CA, with the possibility to track previously created certificates and renew/delete them when required. For more information, see "Support for Automated Certificate Life*cycle Management*" 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. Currently, this feature is implemented only for SM service call flows. For more information, see "*Support for Unique Log Identifier Across Policy Services*" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide.*
- **Trigger TerminateNotify to SMF During Stale Session Cleanup**: SM Service sends TerminateNotify to SMF when it detects and cleans up duplicate requests of SM PDU Session Create (Collision Detection) and stale SMPolicyAssociation (Max TTL reached for session). For more information, see "*Sending Terminate Notify to SMF*" under "*Stale Session Handling*" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.
- **Audit Support for Usage Monitoring Service**: Policy supports stale session detection and cleanup in Usage Monitoring service with the support of Audit service. It identifies the stale sessions based on lastAccessTime. For more information, see "*Stale Session Detection and Handling in Usage Monitoring Service*" under "*Stale Session Handling*" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.
- **PCF Support for ME-XX String in Server Header from CHF**: PCF ignores the server header if a differently formatted value is inserted in the header alongside the 3GPP supported ones. This impacts the session retry strategy. This feature enables PCF core (SM/AM/UE) services to ignore the custom server header values and continue considering the 3GPP standard and valid SCP, SEPP or other NF type server headers format inserted in the header. For more information, see "*PCF Support for ME-XX String in Server Header from CHF*" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.
- **Sy SLR Enhancements for Signaling Updates and UDR Notification**: This feature enables cnPCRF and cnPolicy to fetch OCS counter status over Sy reference point in a synchronous mode on receiving a signaling update or a UDR notification. For more information, see "*Sy SLR Enhancements for Signaling Updates and UDR Notification*" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide.*
- **Binding Service Pod Congestion Control**: Binding service supports Congestion Control mechanism that helps to handle the 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 "*Binding Service Pod Congestion Control*" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*
- **Enhancement to PCF Resiliency:** PCF is enhanced to provide the mechanism in consumer service pods to cache the last successful producer pod information and use it when the subsequent producer pod discovery results in failure. Hence, the inter service communication continues to run even when the communication between the Kubernetes services and pods is down.
- **MultiSelection Capability for Features and Scenarios**: ATS allows users to select and run single or multiple features and scenarios by selecting a check box for the corresponding features or scenarios. For more information, see the "*Multiselection Capability for Features and Scenarios*" section in *Oracle Communications Cloud Native Core, Automated Testing Suite Guide*.
- **Individual Stage Group Selection**: This feature allows users to select and execute a single or multiple stages or groups by selecting a check box for the corresponding stage or group. For more information, see "*Individual Stage Group Selection*" section in *Oracle Communications Cloud Native Core, Automated Test Suite Guide*.

2.12 Service Communication Proxy (SCP)

Release 24.1.2

Oracle Communications Cloud Native Core, Service Communication Proxy (SCP) 24.1.2 has been updated with the following enhancements:

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

Release 24.1.0

Oracle Communications Cloud Native Core, Service Communication Proxy (SCP) 24.1.0 has been updated with the following enhancements:

- **Managing Delegated Discovery Response Caching Based on Query Parameters**: With this enhancement, SCP can perform selective caching of the discovery responses based on the user-configurable discovery query parameter list. Therefore, the selective caching control helps users reduce the risk of cache overflow. This caching mechanism helps to optimize the performance while reducing latency. For more information, see "*Managing Delegated Discovery Response Caching Based on Query Parameters*" in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.
- **Support for Health Status cnDBTier APIs in CNC Console:** With this enhancement, Health Status cnDBTier APIs are integrated into the CNC Console, and users can view the health status of the microservices, such as replication, backup manager, monitor services, and NDB services on the CNC Console. For more information, see "*Support for cnDBTier APIs in CNC Console*" in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.
- **Mediation Log Level Configuration**: With this enhancement, you can fetch and update the log level settings of the mediation service through the REST API by enhancing the operational efficiency of the mediation service. For more information, see "*Mediation Log Level Configuration*" in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.
- **Deployment in OCI using OCI Adaptor**: Oracle Cloud Infrastructure (OCI) is a set of complementary cloud services that enable you to build and run a range of applications and services in a High Availability (HA) hosted environment. SCP can be integrated into the OCI using the OCI Adaptor.
  OCI Adaptor provides a smooth integration to SCP observability and monitoring modules with OCI observability and management, enabling the users to have access of alerts, metrics, and KPIs on the OCI platform.

  For more information on deploying SCP in OCI, see *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*, *Oracle Communications Cloud Native Core, Service Communication Proxy Installation, Upgrade, and Fault Recovery Guide*, and *Oracle Communications Cloud Native Core, OCI Adaptor Reference Architecture Guide*.
- **IPv6 Support**: SCP supports IPv6. You can deploy SCP with IPv4 or IPv6 or both simultaneously. For more information, see "*Dual Stack Support*" in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.
- **Error Response Enhancement**: With the enhanced error response mechanism, SCP sends additional information, such as server FQDN, NF service name, vendor name, and error ID, in the `detail` parameter of `ProblemDetails` to find the specific cause of the error. This helps in error identification and reduces troubleshooting time. For more information, see "*Error Response Enhancement*" in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.

- **NFProfile Processing Enhancements**: With this enhancement, whenever SCP receives a notification regarding an NF profile that includes 3GPP-defined supported NF services, custom, unknown, or unsupported NF services, SCP ignores the presence of custom, unknown, or unsupported NF services within the NF profile. Routing rules are generated by SCP for 3GPP-defined SCP supported NF services that are present in the NF profile. For more information, see "*NFProfile Processing Enhancements*" in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.
- **Message Feed Enhancement**: SCP is enhanced to select Kafka partitions based on the correlation ID `kafkaPartitionSelectionLogic` REST API configuration to distribute the messages to the same or different partitions in a Kafka broker. For more information, see "*Message Feed Enhancements*" in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.
- **SCP-Worker Pod Capacity Improvements**: Per pod capacity of SCP-Worker has been increased. For more information, see *SCP Dimensioning Spreadsheet*.

> **Note:**
>
> Release 15 deployment model is not supported from SCP 24.1.0.

2.13 Security Edge Protection Proxy (SEPP)

Release 24.1.0

Oracle Communications Cloud Native Core, Security Edge Protection Proxy (SEPP) 24.1.0 has been updated with the following enhancements:

- **Deployment in OCI using OCI Adaptor**: Oracle Cloud Infrastructure (OCI) is a set of complementary cloud services that enable you to build and run a range of applications and services in a High Availability (HA) hosted environment. SEPP can be integrated into the OCI using the OCI Adaptor.
  OCI Adaptor provides a smooth integration to SEPP observability and monitoring modules with OCI observability and management, enabling the users to have access of alerts, metrics, and KPIs on the OCI platform. For more information on deploying SEPP in OCI, see *Oracle Communications Cloud Native Core, Security Edge Communication Proxy User Guide* and *Oracle Communications Cloud Native Core, Security Edge Communication Proxy Installation, Upgrade, and Fault Recovery Guide*, and *Oracle Communications Cloud Native Core, OCI Adaptor Deployment Guide*.
- **Support for TLS 1.3:** SEPP supports TLS 1.3 for all functions and interfaces that are supported by TLS 1.2. With this feature, SEPP supports the creation of TLS 1.3 and TLS 1.2 connections and mandatory ciphers and extensions. Network Functions (NFs) or peers can use Hypertext Transfer Protocol Secure (HTTPS) to establish secured ingress and egress connections with consumer NFs and producer NFs, respectively. These communication protocols are encrypted using Transport Layer Security (TLS). TLS comprises the following components:
  - Handshake Protocol: Exchanges the security parameters of a connection. Handshake messages are supplied to the TLS record layer.
  - Record Protocol: Receives the messages to be transmitted, fragments the data into multiple blocks, secures the records, and then transmits the result. Received data is delivered to higher-level peers.

For more information about the feature, see the "*Support for TLS 1.3*" section in *Oracle Communications Cloud Native Core, Security Edge Protection Proxy User Guide* and the

"*Configurable Parameters*" section in *Oracle Communications Cloud Native Core, Security Edge Protection Proxy Installation, Upgrade, and Fault Recovery Guide*.

- **Support for Automated Certificate Lifecycle Management:** In SEPP 23.4.x and earlier, X.509 and Transport Layer Security (TLS) certificates were managed manually. When multiple instances of SEPP were deployed in a 5G network, certificate management, that includes certificate creation, renewal, and removal became tedious and error-prone. Starting with SEPP 24.1.x, SEPP can be integrated with Oracle Communications Cloud Native Core, Certificate Management (OCCM) to support the automation of certificate lifecycle management. OCCM manages TLS certificates stored in Kubernetes secrets by integrating with Certificate Authority (CA) using the Certificate Management Protocol Version 2 (CMPv2) protocol in the Kubernetes secret. OCCM obtains and signs TLS certificates within the SEPP namespace. For more information about OCCM, see the "*Support for Automated Certificate Lifecycle Management*" section in *Oracle Communications Cloud Native Core, Security Edge Protection Proxy User Guide*, and *Oracle Communications Cloud Native Core, Certificate Management User Guide*.
- **Support for Health Status cnDBTier APIs in CNC Console:** With this enhancement, Health Status cnDBTier APIs are integrated into the CNC Console, and users can view specific cnDBTier statuses on the CNC Console. For more information about the feature, see the "*Support for cnDBTier APIs in CNC Console*" and "*cnDBTier*" sections in *Oracle Communications Cloud Native Core, Security Edge Protection Proxy User Guide*.
- **SEPP ATS Deployment in OCI:** This feature allows the users to deploy the SEPP ATS in OCI. For more information about the feature, see the "*ATS Framework Features*" section in *Oracle Communications Cloud Native Core, Automated Testing Suite Guide*.

2.14 Unified Data Repository (UDR)

Release 24.1.1

Oracle Communications Cloud Native Core, Unified Data Repository (UDR) 24.1.1 has been updated with the following enhancements:

- **Suppress Notification**: This feature enables cnUDR to store the User-Agent header received in the POST request from cnPCRF in the subscription table. cnUDR compares the User-Agent header received during an update operation from cnPCRF with the stored User-Agent header. If the User-Agent header match, then the notification is suppressed. The notification is sent if the User-Agent header do not match or if there is no User-Agent header in the update request. For more information about the feature, see "Suppress Notification" section in *Oracle Communications Cloud Native Core, Unified Data Repository User Guide.*

Release 24.1.0

Oracle Communications Cloud Native Core, Unified Data Repository (UDR) 24.1.0 has been updated with the following enhancements:

- **Error response enhancements**: The error responses used to earlier contain only the error description in the details field, which was insufficient to trouble shoot any error. Using the enhanced error response mechanism, UDR sends additional pieces of information such as server FQDN, NF service name, vendor name, and error ID, in the details field of the payload for the identification of the source of an error response. For more information, see "*Error response enhancements*" section *in Oracle Communications Cloud Native Core, Unified Data Repository User Guide.*
- **Support for Provisioning Logs:** This feature enhances the provisioning logging functionality with a logging type that is independent of the logging level. This feature helps

in collecting the subscriber provisioning logs by enabling the provisioning logging mechanism. The operator can also log the 5G subscriber provisioning requests for create, update, and delete operations by enabling the co-relation between request and response. For more information, see "*Support for Provisioning Logs*" section in *Oracle Communications Cloud Native Core, Unified Data Repository User Guide.*

- ***Auditor Service Enhancements****:* The auditor service feature is enhanced by utilizing the SLF subscriber export tool functionality. The SLF subscriber data created across the SLF segments in Comma Separated Value (CSV) file format is transferred to the auditor service using Secure File Transfer Protocol (SFTP). The auditor service accesses and compares the transferred files for discrepancies. The audit report generated is used to identify the discrepancies between the subscriber data stored across the SLF segments. For more information, see "*Auditor Service*" section in *Oracle Communications Cloud Native Core, Provisioning Gateway Guide.*
- **Ingress Gateway Pod Protection**: This feature protects the Ingress Gateway pods from overloading due to uneven traffic distribution, traffic bursts, or congestion. It ensures the protection and mitigation of pods from entering a congestion state condition, while also facilitating necessary actions for recovery. For more information about Ingress Gateway Pod Protection, see "*Ingress Gateway Pod Protection*" in *Oracle Communications Cloud Native Core, Unified Data Repository User Guide*.
- **Support for cnDBTier Health APIs in CNC Console:** With this enhancement, cnDBTier Health APIs are integrated into the CNC Console, and users can view cnDBTier Health status on the CNC Console. For more information, see "*Support for cnDBTier APIs in CNC Console*" 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 3.24.1. 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 3.24.1

Description	NF Version	ATS Version	Upgrade Supported
Oracle Communications Cloud Native Core, Binding Support Function (BSF)	24.1.0	24.1.0	BSF 24.1.0 supports fresh installation and upgrade from 23.4.x. For more information, see *Oracle Communications Cloud Native Core, Binding Support Function Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Configuration Console (CNC Console)	24.1.1	NA	CNC Console 24.1.1 supports fresh installation and upgrade from 24.1.0, 23.3.x and 23.4.x. For more information, see *Oracle Communications Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide*. **Note:** CNC Console supports N-2 NF versions during upgrade window. For example, CNC Console 24.1.x supports SCP 24.1.x, 23.4.x, and 23.3.x. Any newly added features in CNC Console which have NF dependency in latest release may not be available in previous release.
Oracle Communications Cloud Native Configuration Console (CNC Console)	24.1.0	NA	CNC Console 24.1.0 supports fresh installation and upgrade from 23.3.x and 23.4.x. For more information, see *Oracle Communications Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide*.

Table 3-1 (Cont.) Media Pack Contents for Oracle Communications Cloud Native Core 3.24.1

Description	NF Version	ATS Version	Upgrade Supported
Oracle Communications Cloud Native Core, Cloud Native Environment (CNE)	24.1.2	NA	CNE 24.1.2 supports fresh installation and upgrade from 23.4.x and 24.1.x. For more information, see *Oracle Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Cloud Native Environment (CNE)	24.1.1	NA	CNE 24.1.1 supports fresh installation and upgrade from 23.4.x and 24.1.0. For more information, see *Oracle Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Cloud Native Environment (CNE)	24.1.0	NA	CNE 24.1.0 supports fresh installation and upgrade from 23.4.x. For more information, see *Oracle Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Operations Services Overlay (OSO)	24.1.0	NA	OSO 24.1.0 supports fresh installation and upgrade from 23.3.1. For more information, see Oracle Communications Operations Services Overlay Installation and Upgrade Guide.
Oracle Communications Cloud Native Core, Certificate Management (OCCM)	24.1.0	NA	OCCM 24.1.0 supports fresh installation and upgrade from 23.4.x. For more information, see *Oracle Communications Cloud Native Core, Certificate Management Installation, Upgrade, and Fault Recovery Guide.*
Oracle Communications Cloud Native Core, cnDBTier	24.1.2	NA	cnDBTier 24.1.2 supports fresh installation and upgrade from 23.3.x, 23.4.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, cnDBTier	24.1.1	NA	cnDBTier 24.1.1 supports fresh installation and upgrade from 23.3.x, 23.4.x, and 24.1.0. 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 3.24.1

Description	NF Version	ATS Version	Upgrade Supported
Oracle Communications Cloud Native Core, cnDBTier	24.1.0	NA	cnDBTier 24.1.0 supports fresh installation and upgrade from 23.3.x and 23.4.x. For more information, see *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Network Exposure Function (NEF)	24.1.0	24.1.0	NEF 24.1.0 supports fresh installation and upgrade from 23.3.x and 23.4.x. For more information, see *Oracle Communications Cloud Native Core, Network Exposure Function Installation, Upgrade, and Fault Recovery Guide* .
Oracle Communications Cloud Native Core, Network Repository Function (NRF)	24.1.3	24.1.3	NRF 24.1.3 supports fresh installation and upgrade from 23.4.x and 24.1.x. For more information, see *Oracle Communications Cloud Native Core, Network Repository Function Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Network Repository Function (NRF)	24.1.2	24.1.2	NRF 24.1.2 supports fresh installation and upgrade from 23.4.x and 24.1.x. For more information, see *Oracle Communications Cloud Native Core, Network Repository Function Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Network Repository Function (NRF)	24.1.1	24.1.1	NRF 24.1.1 supports fresh installation and upgrade from 23.4.x and 24.1.0. For more information, see *Oracle Communications Cloud Native Core, Network Repository Function Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Network Repository Function (NRF)	24.1.0	24.1.0	NRF 24.1.0 supports fresh installation and upgrade from 23.4.x. For more information, see *Oracle Communications Cloud Native Core, Network Repository Function Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Network Slice Selection Function (NSSF)	24.1.1	24.1.1	NSSF 24.1.1 supports fresh installation and upgrade from 23.4.x and 24.1.0. For more information, see *Oracle Communications Cloud Native Core, Network Slice Selection Function Installation, Upgrade, and Fault Recovery Guide*.

Table 3-1 (Cont.) Media Pack Contents for Oracle Communications Cloud Native Core 3.24.1

Description	NF Version	ATS Version	Upgrade Supported
Oracle Communications Cloud Native Core, Network Slice Selection Function (NSSF)	24.1.0	24.1.0	NSSF 24.1.0 supports fresh installation and upgrade from 23.4.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, OCI Adaptor	24.1.0	NA	OCI Adaptor 24.1.0 supports fresh installation. For more information, see *Cloud Native Core OCI Adaptor, NF Deployment in OCI Guide.*
Oracle Communications Cloud Native Core, Converged Policy (Policy)	24.1.0	24.1.0	Policy 24.1.0 supports fresh installation and upgrade from 23.4.x. For more information, see *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Service Communications Proxy (SCP)	24.1.2	24.1.2	SCP 24.1.2 supports fresh installation and upgrade from 23.3.x, 23.4.x, and 24.1.x. For more information, see *Oracle Communications Cloud Native Core, Service Communication Proxy Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Service Communications Proxy (SCP)	24.1.0	24.1.0	SCP 24.1.0 supports fresh installation and upgrade from 23.3.x and 23.4.x. For more information, see *Oracle Communications Cloud Native Core, Service Communication Proxy Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Security Edge Protection Proxy (SEPP)	24.1.0	24.1.0	SEPP 24.1.0 supports fresh installation and upgrade from 23.3.x and 23.4.x. For more information, see *Oracle Communications Cloud Native Core, Security Edge Protection Proxy Installation, Upgrade, and Fault Recovery Guide.*
Oracle Communications Cloud Native Core, Unified Data Repository (UDR)	24.1.1	24.1.1	UDR 24.1.1 supports fresh installation and upgrade from 23.3.x, 23.4.x, and 24.1.0. For more information, see *Oracle Communications Cloud Native Core, Unified Data Repository Installation, Upgrade, and Fault Recovery Guide*.

Table 3-1 (Cont.) Media Pack Contents for Oracle Communications Cloud Native Core 3.24.1

Description	NF Version	ATS Version	Upgrade Supported
Oracle Communications Cloud Native Core, Unified Data Repository (UDR)	24.1.0	24.1.0	UDR 24.1.0 supports fresh installation and upgrade from 23.3.x, and 23.4.x. For more information, see *Oracle Communications Cloud Native Core, Unified Data Repository Installation, Upgrade, and Fault Recovery Guide*.

3.2 Compatibility Matrix

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

Table 3-2 Compatibility Matrix

CNC NF	NF Version	CNE	cnDBTier	CDCS	OSO	ASM S/W	Kubernetes	CNC Console	OCNADD	OCCM	OCI Adaptor
BSF	24.1.0	• 24.1.x • 23.4.x	• 24.1.x • 23.4.x	NA	• 23.4.x • 23.2.x	1.14.6	• 1.28.x • 1.27.x	• 24.1.x • 23.4.x	NA	24.1.x	NA
CNC Console	24.1.1	• 24.1.x • 23.4.x • 23.3.x	• 24.1.x • 23.4.x • 23.3.x	NA	• 23.4.x • 23.3.x • 23.2.x	• 1.14.6 • 1.11.8 • 1.9.8	• 1.28.x • 1.27.x • 1.26.x	NA	24.1.x	24.1.x	24.1.x
CNC Console	24.1.0	• 24.1.x • 23.4.x • 23.3.x	• 24.1.x • 23.4.x • 23.3.x	NA	• 23.4.x • 23.3.x • 23.2.x	• 1.14.6 • 1.11.8 • 1.9.8	• 1.28.x • 1.27.x • 1.26.x	NA	24.1.x	24.1.x	24.1.x
CNE	24.1.2	NA	NA	NA	NA	NA	1.28.x	NA	NA	NA	NA
CNE	24.1.1	NA	NA	NA	NA	NA	1.28.x	NA	NA	NA	NA
CNE	24.1.0	NA	NA	NA	NA	NA	1.28.x	NA	NA	NA	NA

Table 3-2 (Cont.) Compatibility Matrix

CNC NF	NF Version	CNE	cnDBTier	CDCS	OSO	ASM S/W	Kubernetes	CNC Console	OCNADD	OCCM	OCI Adaptor
cnDBTier	24.1.2	• 24.1.x • 23.4.x • 23.3.x	NA	NA	NA	NA	• 1.28.x • 1.27.x • 1.26.x	NA	NA	NA	24.1.x
cnDBTier	24.1.1	• 24.1.x • 23.4.x • 23.3.x	NA	NA	NA	NA	• 1.28.x • 1.27.x • 1.26.x	NA	NA	NA	24.1.x
cnDBTier	24.1.0	• 24.1.x • 23.4.x • 23.3.x	NA	NA	NA	NA	• 1.28.x • 1.27.x • 1.26.x	NA	NA	NA	24.1.x
OCCM	24.1.0	• 24.1.x • 23.4.x • 23.3.x	NA	• 23.4.x • 23.3.x	NA	NA	• 1.28.x • 1.27.x • 1.26.x	24.1.x	NA	NA	NA
OSO	24.1.0	• 24.1.x • 23.4.x • 23.3.x	NA	NA	NA	NA	• 1.28.x • 1.27.x • 1.26.x	NA	NA	NA	NA
NEF	24.1.0	• 24.1.x • 23.4.x • 23.3.x	• 24.1.x • 23.4.x • 23.3.x	NA	NA	NA	• 1.28.x • 1.27.x • 1.26.x	24.1.x	NA	NA	NA
NRF	24.1.3	• 24.1.x • 23.4.x • 23.3.x	• 24.1.x • 23.4.x • 23.3.x	• 23.4.x • 23.3.x • 23.2.x	23.4.x	1.14.6	• 1.28.x • 1.27.x • 1.26.x	24.1.x	24.1.x	24.1.x	24.1.x

Table 3-2 (Cont.) Compatibility Matrix

CNC NF	NF Version	CNE	cnDBTier	CDCS	OSO	ASM S/W	Kubernetes	CNC Console	OCNADD	OCCM	OCI Adaptor
NRF	24.1.2	• 24.1.x • 23.4.x • 23.3.x	• 24.1.x • 23.4.x • 23.3.x	• 23.4.x • 23.3.x • 23.2.x	23.4.x	1.14.6	• 1.28.x • 1.27.x • 1.26.x	24.1.x	24.1.x	24.1.x	24.1.x
NRF	24.1.1	• 24.1.x • 23.4.x • 23.3.x	• 24.1.x • 23.4.x • 23.3.x	• 23.4.x • 23.3.x • 23.2.x	23.4.x	1.14.6	• 1.28.x • 1.27.x • 1.26.x	24.1.x	24.1.x	24.1.x	24.1.x
NRF	24.1.0	• 24.1.x • 23.4.x • 23.3.x	• 24.1.x • 23.4.x • 23.3.x	• 23.4.x • 23.3.x • 23.2.x	23.4.x	1.14.6	• 1.28.x • 1.27.x • 1.26.x	24.1.x	24.1.x	24.1.x	24.1.x
NSSF	24.1.1	• 24.1.x • 23.4.x • 23.3.x	• 24.1.x • 23.4.x • 23.3.x	NA	23.4.x	1.14.6	• 1.28.x • 1.27.x • 1.26.x	24.1.x	NA	NA	NA
NSSF	24.1.0	• 24.1.x • 23.4.x • 23.3.x	• 24.1.x • 23.4.x • 23.3.x	NA	23.4.x	1.14.6	• 1.28.x • 1.27.x • 1.26.x	24.1.x	NA	NA	NA
Policy	24.1.0	• 24.1.x • 23.4.x	• 24.1.x • 23.4.x	NA	• 23.4.x • 23.2.x	1.14.6	• 1.28.x • 1.27.x	• 24.1.x • 23.4.x	NA	24.1.x	NA
SCP	24.1.2	• 24.1.x • 23.4.x • 23.3.x	• 24.1.x • 23.4.x • 23.3.x	• 23.4.x • 23.3.x	• 23.4.x • 23.3.x	• 1.14.6 • 1.11.8	• 1.28.x • 1.27.x • 1.26.x	24.1.x	24.1.x	24.1.x	24.1.x

Table 3-2 (Cont.) Compatibility Matrix

CNC NF	NF Version	CNE	cnDBTier	CDCS	OSO	ASM S/W	Kubernetes	CNC Console	OCNADD	OCCM	OCI Adaptor
SCP	24.1.0	• 24.1.x • 23.4.x • 23.3.x	• 24.1.x • 23.4.x • 23.3.x	• 23.4.x • 23.3.x	• 23.4.x • 23.3.x	• 1.14.6 • 1.11.8	• 1.28.x • 1.27.x • 1.26.x	24.1.x	24.1.x	24.1.x	24.1.x
SEPP	24.1.0	• 24.1.x • 23.4.x • 23.3.x	• 24.1.x • 23.4.x • 23.3.x	• 23.4.x • 23.3.x	• 23.4.x • 23.3.x	1.14.6	• 1.28.x • 1.27.x • 1.26.x	24.1.x	NA	24.1.x	24.1.x
UDR	24.1.1	• 24.1.x • 23.4.x • 23.3.x	• 24.1.x • 23.4.x • 23.3.x	NA	• 23.4.x • 23.3.x • 23.2.x	• 1.14.6 • 1.11.8	• 1.28.x • 1.27.x • 1.26.x	24.1.x	NA	NA	NA
UDR	24.1.0	• 24.1.x • 23.4.x • 23.3.x	• 24.1.x • 23.4.x • 23.3.x	NA	• 23.4.x • 23.3.x • 23.2.x	• 1.14.6 • 1.11.8	• 1.28.x • 1.27.x • 1.26.x	24.1.x	NA	NA	NA

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.

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	24.1.0	• 3GPP TS 23.501 v17.7.0 • 3GPP TS 23.502 v17.7 • 3GPP TS 23.503 V17.7 • 3GPP TS 29.500 v17.7.0 • 3GPP TS 29.510 v17.7 • 3GPP TS 29.513 V17.7 • 3GPP TS 29.521 v17.7.0 • 3GPP TS 33.501 V17.7.0
CNC Console	24.1.0	NA
CNE	24.1.x	NA
cnDBTier	24.1.x	NA
NEF	24.1.0	• 3GPP TS 29.122 16.10.0, 17.10.0 • 3GPP TS 23.222 16.9.0 • 3GPP TS 23.501 16.10.0 • 3GPP TS 23.502 16.10.0, 17.10.0 • 3GPP TS 29.514 16.10.0, 17.9.0 • 3GPP TS 29.521 16.10 • 3GPP TS 29.503 16.14.0, 17.11.0 • 3GPP TS 29.515 16.7 • 3GPP TS 29.222 16.5.0 • 3GPP TS 29.500 16.6.0 • 3GPP TS 29.501 16.6.0 • 3GPP TS 29.522 16.10.0, 17.10.0 • 3GPP TS 29.510 16.6.0 • 3GPP TS 29.591 16.3.0 • 3GPP TS 29.518 16.14.0, 17.10.0 • 3GPP TS 33.501 17.7.0 • 3GPP TS 29.504 16.10.0 • 3GPP TS 29.519 16.11.0 • 3GPP TS 29.508 16.11.0 • 3GPP TS 23.682 16.9.0 • 3GPP TS 29.337 16.1.0 • 3GPP TS 29.214 16.7.0 • 3GPP TS 32.291 16.14 • 3GPP TS 32.290 16.10.0 • 3GPP TS 32.254 16.6.0 • 3GPP TS 29.338 17.1.0 • 3GPP TS 23.040 17.2.0
NRF	24.1.x	• 3GPP TS 29.510 v15.5 • 3GPP TS 29.510 v16.3.0 • 3GPP TS 29.510 v16.7
NSSF	24.1.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
OSO	24.1.0	NA

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

CNC NF	NF Version	3GPP
OCCM	24.1.0	• 3GPP TS 33.310-h30 • 3GPP TR 33.876 v.0.3.0
Policy	24.1.0	• 3GPP TS 33.501 v17.7.0 • 3GPP TS 29.500v16.9.0 • 3GPP TS 23.501v16.9.0 • 3GPP TS 23.502v16.9.0 • 3GPP TS 23.503v16.9.0 • 3GPP TS 29.504v16.9.0 • 3GPP TS 29.507v16.9.0 • 3GPP TS 29.510v16.9.0 • 3GPP TS 29.512v16.14 • 3GPP TS 29.513v16.9.0 • 3GPP TS 29.514v16.14.0 • 3GPP TS 29.214v16.5.0 • 3GPP TS 29.518v16.13.0 • 3GPP TS 29.519v16.8 • 3GPP TS 29.520v16.8 • 3GPP TS 29.521v16.8.0 • 3GPP TS 29.525v16.9.0 • 3GPP TS 29.594v16.7 • 3GPP TS 23.203 v16.2.0 • 3GPP TS 29.212 V16.3.0 • 3GPP TS 29.213v16.3 • 3GPP TS 29.214 v16.2.0 • 3GPP TS 29.219 v16.0.0 • 3GPP TS 29.335v16.0
SCP	24.1.0	3GPP TS 29.500 R16 v16.6.0
SEPP	24.1.0	• 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	24.1.x	• 3GPP TS 29.505 v15.4.0 • 3GPP TS 29.504 v16.2.0 • 3GPP TS 29.519 v16.2.0 • 3GPP TS 29.511 v17.2.0

Note:

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

3.4 Common Microservices Load Lineup

This section provides information about common microservices and ATS for the specific NF versions in Oracle Communications Cloud Native Core Release 3.24.1.

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	24.1.0	24.1.5	24.1.4	24.1.0	24.1.1	24.1.4	24.1.1	24.1.5	24.1.5	24.1.1	NA	24.1.5	24.1.4
CNC Console	24.1.1	NA	NA	NA	NA	NA	24.1.3	NA	24.1.10	24.1.2	NA	NA	NA
CNC Console	24.1.0	NA	NA	NA	NA	NA	24.1.1	NA	24.1.5	24.1.1	NA	NA	NA
NEF	24.1.0	NA	24.1.2	NA	24.1.1	24.1.2	24.1.1	24.1.4	24.1.4	24.1.1	NA	24.1.5	24.1.2
NRF	24.1.3	24.1.9	24.1.3	24.1.0	24.1.1	NA	24.1.1	24.1.9	24.1.9	24.1.1	NA	NA	24.1.3
NRF	24.1.2	24.1.9	24.1.3	24.1.0	24.1.1	NA	24.1.1	24.1.9	24.1.9	24.1.1	NA	NA	24.1.3
NRF	24.1.1	24.1.7	24.1.3	24.1.0	24.1.1	NA	24.1.1	24.1.7	24.1.7	24.1.1	NA	NA	24.1.3
NRF	24.1.0	24.1.5	24.1.3	24.1.0	24.1.1	NA	24.1.1	24.1.5	24.1.5	24.1.1	NA	NA	24.1.3
NSSF	24.1.1	24.1.6	24.1.3	24.1.0	24.1.1	24.1.3	24.1.1	24.1.6	24.1.6	24.1.1	NA	24.1.5	24.1.3
NSSF	24.1.0	24.1.6	24.1.3	24.1.0	24.1.1	24.1.3	24.1.1	24.1.6	24.1.6	24.1.1	NA	24.1.5	24.1.3
OCCM	24.1.0	NA	NA	NA	NA	NA	24.1.1	NA	NA	24.1.1	NA	NA	NA
Policy	24.1.0	24.1.5	24.1.4	24.1.0	24.1.1	24.1.4	24.1.1	24.1.5	24.1.5	24.1.1	NA	24.1.5	24.1.4
SCP	24.1.2	NA	NA	24.1.0	24.1.2	NA	24.1.2	NA	NA	24.1.1	24.1.1	NA	NA
SCP	24.1.0	NA	NA	24.1.0	24.1.1	NA	24.1.1	NA	NA	24.1.1	24.1.0	NA	NA
SEPP	24.1.0	24.1.5	24.1.3	24.1.0	24.1.1	24.1.3	24.1.1	23.4.5	24.1.5	24.1.1	24.1.0	24.1.5	24.1.3
UDR	24.1.1	24.1.8	24.1.3	24.1.0	24.1.1	24.1.3	24.1.1	24.1.8	24.1.8	24.1.1	NA	24.1.5	24.1.3
UDR	24.1.0	24.1.5	24.1.3	24.1.0	24.1.1	24.1.3	24.1.1	24.1.5	24.1.5	24.1.1	NA	24.1.5	24.1.3

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 24.1.0

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	Mar 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	Mar 06, 2024	No unmitigated critical or high findings
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	Mar 21, 2024	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	Apr 22, 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 24.1.1

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	Feb 28, 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	Feb 28, 2024	No unmitigated critical or high findings
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	Apr 15, 2024	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	Apr 16, 2024	No findings

Release 24.1.0

Table 3-7 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	Feb 28, 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	Feb 28, 2024	No unmitigated critical or high findings

Table 3-7 (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	Apr 15, 2024	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	Apr 16, 2024	No findings

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

3.5.3 NRF Security Certification Declaration

Release 24.1.3

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	August 13, 2024	No unmitigated critical or high findings
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	August 13, 2024	No unmitigated critical or high findings
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	August 13, 2024	No unmitigated critical or high finding

Table 3-8 (Cont.) NRF 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	August 13, 2024	No findings

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

Release 24.1.2

Table 3-9 NRF Security Certification Declaration

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

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

Release 24.1.1

Table 3-10 NRF Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	May 30, 2024	No unmitigated critical or high findings
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	May 30, 2024	No unmitigated critical or high findings
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	May 30, 2024	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	May 30, 2024	No findings

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

Release 24.1.0

Table 3-11 NRF Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	Mar 1, 2024	No unmitigated critical or high findings

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

Compliance Test Description	Test Completion Date	Summary
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	Mar 1, 2024	No unmitigated critical or high findings
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	Mar 1, 2024	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	Mar 1, 2024	No findings

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

3.5.4 NEF Security Certification Declaration

Release 24.1.0

Table 3-12 NEF Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	Apr 17, 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	Feb 19, 2024	No unmitigated critical or high findings

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

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

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

3.5.5 NSSF

Release 24.1.1

Table 3-13 NSSF Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	June 8, 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	June 8, 2024	No unmitigated critical or high findings
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	June 8, 2024	No unmitigated critical or high finding

Table 3-13 (Cont.) NSSF Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	June 8, 2024	No findings

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

Release 24.1.0

Table 3-14 NSSF Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	Mar 1, 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	Mar 1, 2024	No unmitigated critical or high findings
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	Mar 1, 2024	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	Mar 1, 2024	No findings

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

3.5.6 OCCM Security Certification Declaration

Release 24.1.0

Table 3-15 OCCM Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	Apr 12, 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	Feb 29, 2024	No unmitigated critical or high findings
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	Apr 12, 2024	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	Apr 16, 2024	No findings

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

3.5.7 Policy Security Certification Declaration

Policy 24.1.0

Table 3-16 Policy Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	Mar 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	Mar 06, 2024	No unmitigated critical or high findings
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	Mar 21, 2024	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	Apr 22, 2024	No findings

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

3.5.8 SCP Security Certification Declaration

SCP 24.1.2

Table 3-17 SCP Security Certification Declaration

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

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

SCP 24.1.0

Table 3-18 SCP Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	April 13, 2024	No unmitigated critical or high findings

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

Compliance Test Description	Test Completion Date	Summary
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	April 13, 2024	No unmitigated critical or high findings
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	April 13, 2024	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	April 13, 2024	No findings

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

3.5.9 SEPP

Release 24.1.0

Table 3-19 SEPP Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	Mar 7, 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	Mar 7, 2024	No unmitigated critical, high, medium, and low findings. Scan done through RestFuzz.

Table 3-19 (Cont.) SEPP Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	Mar 7, 2024	No unmitigated critical or high findings. Scan done through Blackduck.
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	Mar 7, 2024	No issues found. Scan done through McAfee.

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

3.5.10 UDR

UDR 24.1.1

Table 3-20 UDR Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	Feb 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	Feb 29, 2024	No unmitigated critical or high findings
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	Mar 7, 2024	No unmitigated critical or high finding

Table 3-20 (Cont.) UDR 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	Mar 6, 2024	No findings

UDR 24.1.0

Table 3-21 UDR Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	Feb 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	Feb 29, 2024	No unmitigated critical or high findings
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	Mar 7, 2024	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	Mar 6, 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) 3.24.1 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 3.24.1.

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 3.24.1.

4.2.1 BSF Resolved Bugs

Table 4-1 BSF 24.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35781973	BSF 23.2.0 Missing COMCOL-TC file for SNMP trap MIB definition	COMCOL-TC file was missing for SNMP trap MIB definition in the custom templates.	3	23.2.0
36178281	SYSTEM_OPERATIONAL_STATE_NORMAL alert is not getting cleared.	`SYSTEM_OPERATIONAL_STATE_NORMAL` alert was not getting cleared when the HTTP and DIAMETER traffic was running in a normal state.	3	23.2.3
35830305	BSF sending PUT and PATCH request	BSF was sending PUT and PATCH request in the same body during the same period of time.	4	23.1.0

Note:

Resolved bugs from 23.2.4 and 23.4.2 have been forward ported to Release 24.1.0.

Table 4-2 BSF ATS 24.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
36334250	UnexpectedBSF_ATS_23.4.0 behavior of service account in stub deployment	There was an unexpected creation of service accounts despite configuring the ServiceAccount.create parameters as false in the values.yaml file of ocstub-py.	4	23.4.0

4.2.2 CNC Console Resolved Bugs

Table 4-3 CNC Console 24.1.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37358523	High Memory usage observed with mcore-ingress-gateway pod and the logs showing "java.lang.OutOfMemory Error"	High memory usage was observed with the mcore-ingress-gateway pod, and the logs showed "java.lang.OutOfMemory Error".	2	24.1.0
37358412	Post CNCC upgrade from 23.2.1 to 23.4.2 cnDBTier replication is down.	After the CNCC upgrade from 23.2.1 to 23.4.2, the cnDBTier replication was down. Replication was failing due to DML and DDL commands being executed out of order on replicated sites.	2	23.4.2
37358606	CNCC 23.4: Issue enabling IAM Keycloak logs.	There was an issue enabling IAM Keycloak logs.	3	23.4.1
37358456	Changing settings for the IAM admin user via REST API.	Settings for the IAM admin user were changed via the REST API.	3	23.4.0
37355796	Exceeding length for Route_path in CNCC metrics causing OSO prom-svr crashing after CS-AMPCF/DB/CNCC upgrade to 23.4.x.	The length for Route_path in CNCC metrics exceeded the limit, causing the OSO prom-svr to crash after the CS-AMPCF/DB/ CNCC upgrade to 23.4.x.	3	23.4.0
37358799	CNCC PDB ALLOWED DISRUPTIONS 0 - Kubernetes Upgrade fail.	The CNC C PDB ALLOWED DISRUPTIONS was set to 0, causing the Kubernetes upgrade to fail.	3	24.1.0
37358495	IAM GUI cannot delete User Credentials.	The CNC IAM GUI could not delete user credentials.	4	24.2.0

Table 4-4 CNC Console 24.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36277895	Incorrect expression used for CnccCoreMemoryUsageCrossedCriticalThreshold alert	The expression used for the `CnccCoreMemoryUsageCrossedCriticalThreshold` alert was incorrect.	3	23.4.0
36197792	Clarity regarding the occncc_custom_configtemplates_<marketing-release-number>.zip in the documentation	References to occncc_custom_configtemplates_<marketing-release-number>.zip and CSAR package had to be updated.	3	23.4.0
36410620	Could not find the resource that you are looking for" choosing user in Master Realm	The customer encountered the "Could not find the resource that you are looking for" error when they tried to select a user in the Master Realm if the CNC Console GUI.	3	23.4.0
36419158	IPv6 not working on CNC Console	During the installation of CNC Console 23.4.0, users found that the IPv6 IPs were not assigned, and the CNC Console pods continued to point to IPv4.	3	23.4.0
36445593	CNCC does not show some NFs	Some NFs were not available in the Select Cluster drop-down on the CNC Console GUI.	3	23.4.0
36275224	CNCC 23.4 user guide documentation errors	There was a spelling error in the CNC Console User Guide.	4	23.4.0
36229762	Restore Procedure needs updating/ clarifying	The Fault Recovery DB Backup and Restore procedure needed to be updated for better clarity.	4	23.4.0

Note:

Resolved bugs from 23.4.1 have been forward ported to release 24.1.0.

4.2.3 cnDBTier Resolved Bugs

Table 4-5 cnDBTier 24.1.2 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
36843557	cnDBtier 23.3.1 Not able to restore the Database from the DB backup	cnDBTier wasn't able to restore the database from the database backup as `ndbmtd` pods were not reinitialized when there was a change in certain configurations.	2	23.3.1
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	23.3.1
37019697	Unable to run recovery using dbtrecover script on a setup deployed with pod and container prefix	Georeplication recovery using `dbtrecover` script did not work on setups that were deployed with pod and container prefix.	2	24.3.0
37173763	dbtrecover not marking all down sites as FAILED	The `dbtrecover` script didn't update the status of all failed sites as FAILED.	2	24.3.0
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 4-5 (Cont.) cnDBTier 24.1.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
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
36839653	Error logs observed on terminal on running dbtremovesite script	The `dbtremovesite` script failed when the script was run on deployments where encryption was enabled.	3	24.2.0
36492775	CNCC GUI does not show Service status as down for Backup Manager service when DB connectivity goes down with mysql pods in CNDB 24.1.0rc6	CNC Console GUI did not show service status as `DOWN` for the backup manager service when the database connectivity with MySQL pods got disconnected.	3	24.1.0
36745830	cnDbtier user guide procedure to enable https over replication service is not working	User requested to document the procedure to generate PKCS12 certificate for HTTPS connection between replication services.	3	23.2.3
36930424	Incorrect indentation for Alert: REPLICATION_SVC_STORAGE_FULL in alert rules YAML file	The `REPLICATION_SVC_STORAGE_FULL` alert had incorrect indentation in alert rules YAML file.	3	23.4.6
36942082	24.2.0 cnDBtier alert rules against documentation discrepancies	Duplicate SNMP IDs were observed for alerts in the alert rules YAML file and cnDBTier user guide.	3	24.2.0
37028162	Same OID Used for Alerts 'High CPU' and 'BINLOG_STORAGE_LOW' with Different Severities	Duplicate SNMP IDs were observed for alerts in the alert rules YAML file and cnDBTier user guide.	3	24.3.0
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
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

Table 4-5 (Cont.) cnDBTier 24.1.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
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
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
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
37144276	DBTier 24.2.1 Network policies - Incorrect pod selector for ndbmysqld	Incorrect pod selector was observed for `ndbmysqld` pods when network policy was enabled.	4	24.2.1

Table 4-6 cnDBTier 24.1.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36569659	Site addition failing on a setup deployed with Prefix	Details about supported topologies for `ndb_restore` were not provided in cnDBTier documentation.	2	24.1.0
36610826	Password change not getting triggered	The `dbtpasswd` script didn't support NF password change when capital letters were used in the username and password sub-strings.	2	24.1.0
36610763	Password change not working for NF	`occneuser` was not used as the main user in the `dbtpasswd` script.	2	24.1.0
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
36644058	PCF 6 DB Repl replication_info database not listing all sql host channels between site 2&3	Georeplication broke when running any Data Definition Language (DDL) statement on multichannel cnDBTier deployed with a pod prefix.	2	23.4.3
36575575	Replication break observed on 4 site 6 channel setup post user creation	Replication broke after user creation on the multichannel cnDBTier setups deployed with pod prefix.	2	24.1.0

Table 4-6 (Cont.) cnDBTier 24.1.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36779318	ndbmysqld pod is restarted with EXIT Code 2 during traffic run	Biglog purging logic failed to read decimal value when decimals numbers were used in the disk size of ndbmysqld pods.	3	24.2.0
36688177	dbtrecover script failing on setup with pod and container prefix	Georeplication recovery using the `dbtrecover` script failed when the setups were configured with pod prefix.	3	24.2.0
36502572	DBTier 23.4.2 dbtrecover script failling for multichannel deployment	The `dbtrecover` script failed to perform fault recovery when the system failed to communication from ndbappmysqld pod to remote site loadbalancer IP address of ndbmysqld pods.	3	23.4.2
36517463	dbtrecover script continues execution post error "contact customer support to recover."	User requested to correct misleading error messages in the `dbtrecover` script output.	3	24.1.0
36689742	During stage 2 of conversion misleading errors are observed	Conversion script displayed incorrect error message during stage 2 and stage 3.	3	24.1.0
36557242	RestFuzz analysis on unexpected HTTP responses	cnDBTier returned incorrect HTTPS responses: • The system displayed the 404 error code instead of 500 when server IDs did not exist. • The system displayed the 503 or 404 error code instead of 500 in a single site setup. • The system displayed the 404 error code when "backup_id" was not found in the backup transfer REST API response.	3	24.1.0
36570453	With MTA disabled config replication svc logs displaying MTA as enabled	The replication service created MTA enabled logs even when MTA was disabled.	3	24.1.0
36618788	CNDBTier SNMP alerts: Remote site name not present in description of two alerts	Remote site name was not present in description of two alerts.	3	24.1.0
36515531	CNDB- For ndbappmysqld pods PVC health status shows NA even when pvchealth for ndbapp is set as a true	PVC health status was not supported for ndpapp pods. When users set the `pvchealth` parameter for the unsupported pod (ndbapp), the status was displayed as "NA".	3	24.1.0
36567611	DB Tier Switch Over and Stop Replica API not working without "-k" flag	The CURL commands mentioned in cnDBTier documents had "`-k`" flag which can compromise the security of the system.	3	24.1.0
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

Table 4-6 (Cont.) cnDBTier 24.1.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36486292	BACKUP_TRANSFER_IN_PROGRESS alert retained on setup post remote transfer	`remote_transfer_status` didn't get updated in the database even though the backup transfer was successful. As a result, the `BACKUP_TRANSFER_IN_PROGRESS` alert was retained on setup ever after the remote transfer was completed.	3	24.1.0
36408701	500 Error returned for Replication Health Status when 1 of the replication service goes down in a 4 site GR setup. 24.1.0rc5 build	Replication health status returned the 500 error code, when one of the replication services went down in a three or four-site georeplication setup.	3	24.1.0
36492775	CNCC GUI does not show Service status as down for Backup Manager service when DB connectivity goes down with mysql pods in CNDB 24.1.0rc6	CNC Console GUI did not show service status as DOWN for the backup manager service when the database connectivity with MySQL pods got disconnected.	3	24.1.0
36482364	No RemoteTransferStatus displayed while the backup is being transferred from data pod to replication svc	CNC Console GUI didn't display `RemoteTransferStatus` when the backup was transferred from the data pod to the replication service.	3	24.1.0
36644321	RestFuzz scan results flagged 500 Response codes	The following RestFuzz scan results flagged 500 response codes: • REPLICATION_SVC_RESTFUZZ_SCAN • MONITOR_SVC_RESTFUZZ_SCAN • BACKUP_MANAGER_SVC_RESTFUZZ_SCAN • BACKUP_EXECUTOR_SVC_RESTFUZZ_SCAN	3	23.4.4
36660329	PCF DB 6 Replication - Users and Grants not replicated across sites	The installation guide did not cover the information that users and grants are not replicated to remote sites when multiple replication channels are configured.	3	23.4.3
36723676	cnDBtier 23.3.1 Observing connection error on db-monitor-svc for replication pod. - Lab	Monitor service was unable to call replication service API if the replication port was changed to any port other than 80.	3	23.3.1
36484876	On a non-GR setup constant errors are coming for DbtierRetrieveBinLogSizeMetrics and DbtierRetrieveReplicationMetrics in cndb monitor service	Errors were observed in non-georeplication setups for `DbtierRetrieveBinLogSizeMetrics` and `DbtierRetrieveReplicationMetrics` in the monitor service.	3	24.1.0
36753759	Alert: BACKUP_PURGED_EARLY not coming on prometheus	The `BACKUP_PURGED_EARLY` alert did not appear on Prometheus as the alert condition was incorrect.	3	24.2.0

Table 4-6 (Cont.) cnDBTier 24.1.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36594743	DBTRecover and DBTPassword version doesn't match with CnDB version	The script versions of `dbtrecover` and `dbtpasswd` scripts didn't match with the cnDBTier version.	4	24.1.0
36599370	Enhance DBTRecover logs to point to exact cause of failure.	User requested to correct misleading error messages in the `dbtrecover` script output.	4	24.1.0

Table 4-7 cnDBTier 24.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36271935	Unable to do recovery with DBTRecover as wrong IP is being read in DBTRecover.	The `dbtrecover` script used old IPs to restart the `db-replication-svc` pods.	2	23.4.0
36225991	Restart observed in all replication svc pods while deploying a 3 site 6 channel setup	User requested to add startup probe waiting time parameters in the `custom_values.yaml` file for the replication service pod.	3	23.4.0
35657461	Multiple Restarts observed in ndbmysqld pods during upgrade to 23.2.1	Replication SQL pod restarted before it came up and connected to the cluster when Aspen Mesh service was enabled.	3	23.2.1
34997129	Clarification on DBTier Automated Backup behavior	The timezone for the backup manager service and the executor service had to be changed to UTC timezone.	3	22.4.0
36242316	DBTier DR Script failing, unexpected number of server IDs	User requested to document the procedure to remove a site from a cnDBTier deployment. For the procedure to remove a site from a cnDBTier deployment, see *Oracle Communications Cloud Native Core, cnDBTier User Guide*.	3	23.2.2
36339825	Export variables used from OCCNE	Users used OCCNE_NAMESPACE to perform cnDBTier procedures which wiped out CNE resources. To inform users to perform steps only on cnDBTier namespace, notes are added in the cnDBTier documents wherever necessary.	3	23.4.0
36265057	Error logs observed on terminal when password script is executed with actual NF	Error logs were observed while running the dbtpasswd script. The dbtpasswd script is enhanced to provide better error handling and to roll back changes when an error occurs.	3	23.4.0
36295676	cnDBTier 23.4.0 Replication svc pod in Init state after upgrade from 23.2.1	The init container of "db-replication-svc" failed to start when the primary host included a prefix containing digits.	3	23.4.0

Table 4-7 (Cont.) cnDBTier 24.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36069403	Logging need to be enhanced to report correct logging level and report correct misconfiguration parameter	User requested to improve the log message in the replication service to provide more information about the error.	3	23.1.0
36289873	DBtier 23.4.0 User Guide Recommendations	User requested for details about metrics' dimensions and per-fragment metrics in *Oracle Communications Cloud Native Core, cnDBTier User Guide*.	4	23.4.0
36401678	DBTier 23.4.0 Clarification in Installation Guide about enableInitContainerForIpDiscovery	User requested more clarification in the `enableInitContainerForIpDiscovery` parameter documentation.	4	23.4.0
36076830	Remove duplicate attribute from alerts	Some of the cndBTier alerts contained duplicate attributes referring to `db-monitor-svc`.	4	23.2.3

Note:

Resolved bugs from 23.4.2 have been forward ported to Release 24.1.0.

4.2.4 CNE Resolved Bugs

Table 4-8 CNE 24.1.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36958805	Bastion failover not working with slow network speed to central repo	The Bastion HA switchover failed due to slow image transfer from CENTRAL_REPO host.	2	23.4.4
37161841	Security groups are removed from the ports during switchover	After swo test that forces the old active lbvm to stay in failed state (such as powering down the VM hypervisor), the swo is successful but the ports d not includes the Security Groups cluster_name>-mbips-egress-nat-sg or <cluster_name>-mbips-ext-sg associated to the ports.	2	23.4.1

Table 4-8 (Cont.) CNE 24.1.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36764539	Different private interface names to cause failure	The private internal interface name for all servers (bastion/node/lbvm/master) was ens192. From release 23.3.x, the private internal interface names were changed from ens 192 to ens160 after the OS installation on VMware clusters. The value of private_lbvm_interface is hardcoded from ens192 to ens160. In CNE 24.1.x and OL9.4, there was a private_lbvm_interface failure as the internal interface name was ens192 instead of ens160.	3	24.1.0
36877689	lb-controller fails to install egress NAT rules on LBVM	The private internal interface name for all servers (bastion/node/lbvm/master) was ens192. From release 23.3.x, the private internal interface names were changed from ens 192 to ens160 after the OS installation on VMware clusters. The value of private_lbvm_interface is hardcoded from ens192 to ens160. In CNE 24.1.x and OL9.4, there was a private_lbvm_interface failure as the internal interface name was ens192 instead of ens160.	3	24.1.0

Table 4-8 (Cont.) CNE 24.1.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36975460	exabgp.conf file not getting configured in occne-lb-controller pod	The `exabgp.conf` file does not include the neighbor list. The code in the lb controller, which created a child process to configure the `exabgp.conf` file, failed but the parent was not aware of this failure. The parent continued to run and the lb controller pod came up with the incomplete neighbor list in the `exabgp.conf` file.	3	24.1.0
36893817	intermittent connectivity issue to LoadBalancer service	After deploying the CNE cluster, the `cluster_test` failed as the service IPs from the Bastion host were unreachable. The ARP entry for gateway (ToR switches VRRPv3 VIP) was missing while running the tcpdump.	3	23.4.4
36937440	Opensearch master nodes PVC getting full	Opensearch master nodes were getting created with role of "master,data". This caused master nodes to act as data nodes. OCCNE configuration offered master node only for cluster management because of which node.roles value must be changed to "master" from "master,data".	3	23.4.4
37094904	rook-ceph-OSD Total pod's are not coming up post worker node reboot	When nodes were rebooted, it was not guaranteed that Linux devices (during discovery) will be assigned with the same id. This caused rook-ceph pods failed to come up. This was a bug in rook ceph. rook version uplift fixed the bug.	3	24.2.0

Table 4-8 (Cont.) CNE 24.1.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37121745	lb-controller database has inconsistency with the deployed LoadBalancer services	When *ingress_network_daemon.service* was in failed state, it caused lb-controller database inconsistency with the deployed LoadBalancer services.	3	24.1.0

Table 4-9 CNE 24.1.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36316652	Bastion DNS forwarders failing to resolve openstack auth to worker nodes (DNSsec issue)	Bastion DNS forwarders failed to resolve OpenStack authentication to worker nodes (DNSsec issue).	3	23.4.0
36319935	DNS Server Failure sent from bastion to worker nodes	When observed from Packet Capture (PCAP) trace, the external server responded to the DNS query, however issue raised when the Bastion transferred this response to Kubernetes worker nodes.	3	23.4.0
36569672	Not clearing "DEPLOY IN PROGRESS" banner after addition of WK	The "`DEPLOY IN PROGRESS`" banner did not clear after the addition of a worker node.	3	23.4.1
36566080	CNE Kubernetes Cluster Dashboard" shows incorrect status for 'Nodes Ready' and 'Nodes Not Ready' panels in grafana	Kubernetes cluster dashboard in Grafana displayed incorrect status for 'Nodes Ready' and 'Nodes Not Ready' panels.	3	24.1.0
36573356	OCCNE: , Metrics for cluster disk usage shows no data.	After an upgrade from 23.4.0 to 24.1.0, the metrics for cluster disk usage did not show any data.	3	24.1.0

Table 4-10 CNE 24.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36496165	OCCNE upgrade issue from 23.3.3 to 23.4.1	The code in the `setupUpgrade` (only run on first entry) function of the `upgrade.sh` script did not quote the LBVM string variables. This caused the setting of the variable to include only the first entry (lbvm) in the string causing upgrade issues.	1	23.4.1
36125787	genLbCtrlData.py running on lb Controller fails to generate egress data	While running the `genLbCtrlData.py` script on the lb controller to generate the `lbCtrlData.json` file, the script uses the `OCCNE_vCNE` variable to track if the script is called for OpenStack or VCD. The `genLbCtrlData.py` script skipped the egress data generation completely when the `OCCNE_vCNE` variable was not set.	2	23.2.5
36471284	Stage2 of OCCNE Upgrade from 23.2.5 to 23.3.3 failing	During a switchover, the recreate port logic failed in 23.3.x, 23.4.x, and 24.1.x.	2	23.3.3
36059773	OCCNE Remove Worker Node is failing due to multiple OSD ID	The script to remove a worker node in a BareMetal deployment failed when run using CDCS.	3	23.4.0
35426047	removeWorkerNode.py not targeting node (Openstack)	The maintenance procedure to automatically remove a Kubernetes worker node did not target the specific node (passed as an argument) while calling Terraform.	3	23.2.0

Table 4-10 (Cont.) CNE 24.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36308260	KVM no longer accepts 'ol9' as an os-variant, causes bare-metal deploy failure	CNE BareMetal deployment created Virtual Machines (VM) using theKernel-based Virtual Machine (KVM) os-variant parameter 'ol9'. This os-variant is no longer valid in the latest OL9 update of KVM. As a result, CNE 23.4.x deployment on BareMetal failed when the first VM was created after os_update (usually master-1, as it resides in most systems on host-1 with bastion-1).	3	• 23.4.0 • 23.4.1
36068408	Grafana issues seen in 23.4.0	Many panels in Grafana dashboards did not work as the metric expressions used for those channels were deprecated or updated.	3	23.4.0

Note:

Resolved bugs from 23.2.6, 23.3.4, and 23.4.1 have been forward ported to release 24.1.0.

OSO 24.1.0 Resolved Bugs

There are no resolved bugs in this release.

Note:

Resolved bugs from 23.3.x have been forward ported to Release 24.1.0.

4.2.5 NEF Resolved Bugs

Table 4-11 NEF 24.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36402372	NEF 2 Site GR :IN service solution Upgrade :950tps:- During Site1 CNDB upgrade from 23.4.2 to 24.1.0.rc.5 Replication broken	During Site 1 CNDB in-service solution upgrade from 23.4.2 to 24.1.0, a broken replication was observed.	2	23.4.0
36347442	Due to the pod's delayed readiness, the service device trigger is getting unpublished in the capif	In CAPIF, the Device Trigger service was getting unpublished due to the pod's delayed readiness.	2	23.4.0
36430273	Although GPSI is not a Mandatory parameter,NEF is rejecting the notification scenario where GPSI was missing with code 400	While performing external group subscription,NEF was rejecting the notification scenarios where GPSI was missing with code 400.	3	24.1.0
36315657	"reachabilityType" SMS not supported for GET Operation for "monitoringType" is "UE_REACHABILITY"	When `monitoringType` was set to UE_REACHABILITY, the `reachabilityType` SMS was not supported for GET operation.	3	23.4.0
36315538	Few alerts were missing from 23.4.0 NEFAlertsrules.yaml	Some of the latest alerts were missing from the shared 23.4.0 NEF `alertsrules.yaml` custom file.	3	23.4.0
36300288	Metrics for NEF CHF which are received are different from those that are mentioned in the user doc	Latest metrics information was missing in the *Oracle Communications Cloud Native Core, Network Exposure Function User Guide*.	3	23.4.0
36262516	6.1 NEF Metrics :ME Service Metrics : Method parameters are incorrect.	Latest parameter information was to be updated in ME Service metrics information in the *Oracle Communications Cloud Native Core, Network Exposure Function User Guide*.	3	23.4.0

Table 4-11 (Cont.) NEF 24.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36261116	5.6.4 Update ME Subscription: Table 5-33 Request Body Parameters Description table is not aligned and "#unique_85" link not available	The following issues were identified in the Oracle Communications Cloud Native Core, Network Exposure Function User Guide under Monitoring Events section: • Description column of Request Body Parameters table was not properly aligned. • There was a broken hyperlink in a note.	3	23.4.0
36261284	5.6.4 Update ME Subscription: PUT Operation: URI: {scsAsId} should be replaced by {afId}	In Monitoring Event Subscription section in *Oracle Communications Cloud Native Core, Network Exposure Function User Guide*, the URI for PUT operation needed to be updated with {afId} instead of {scsAsId}.	3	23.4.0
36262043	5.6.4 Update ME Subscription: cURL Command and "monitorExpireTime" value should be corrected	In Monitoring Event Subscription section in *Oracle Communications Cloud Native Core, Network Exposure Function User Guide*, cURL Command and `monitorExpireTime` parameter value needed to be updated.	3	23.4.0
36261425	5.6.4 Update ME Subscription: Some of the parameters data type are not as per 3gpp standard,	In Monitoring Event Subscription section of User Guide, the attributes data type needed to be updated as per 3GPP standards.	3	23.4.0

Table 4-11 (Cont.) NEF 24.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36254900	ME Update procedure supports only "200" code not "201" success code as per 3gpp standard	In Monitoring Event Update section in *Oracle Communications Cloud Native Core, Network Exposure Function User Guide*, the response code was to be updated as per 3GPP standard.	3	23.4.0
36146540	NEF-GR Site:3.6ktps: Mixed traffic(ME,TI and QOS) :During Performance Long run(3 days run) Replication broken and recovered after 15hrs	During performance long run (upto 3 days run), it was identified that replication was broken and recovered after 15 hours.	3	23.4.0
36146349	NEF-GR Site:3.6ktps: Mixed traffic(ME,TI and QOS) :During Performance Long run(3 days run) ndbappmysqld-1 and ndbmysqld-0 pod restarted one time at site1-cndb1.	During long performance run (upto 3 days run), it was identified that ndbappmysqld-1 and ndbmysqld-0 PODs restarted once.	3	23.4.0
36113463	NEF 2 Site GR :IN service solution Upgrade :950tps:- During Site2 CNDB upgrade from 23.3.1 to 23.4.0 Replication broken	During Site2 CNDB upgrade from 23.3.1 to 23.4.0, a broken replication was identified.	3	23.4.0
36107268	Even when the event-type is incorrect, the notification is sent successfully.	NEF was accepting Monitoring Event notifications with incorrect event type.	3	23.4.0
36107121	NEF is rejecting the notification although notification was sent with GPSI when the subscription is done using EXTERNAL-GROUPID	It was identified that NEF was rejecting Monitoring Event notifications, even when the subscription was done using EXTERNAL-GROUPID and the notification was sent with GPSI.	3	23.4.0
35954123	NEF:23.3.1:AFsession QOS:supportedFeatures values are incorrect during QOS subscription	The supportedFeatures value of AFsessionQOS is always "7C", which did not match the value configured in database.	3	23.1.1

Table 4-11 (Cont.) NEF 24.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35897713	Stats for TI and DT are missing in Grafana dashboards of 23.3.0	The Traffic Influence and Device Trigger feature statistics were missing from the Grafana dashboard.	3	23.3.0
35897533	In the long performance runs, Qos and TI traffic is dipping down at periodic intervals due to increase in latency	Due to increase in latency, the long performance runs for AFSessionWithQos and TrafficInfluence flow traffic were dipping down at periodic intervals.	3	23.3.0
35763445	NEF:GRsite:0.5ktps:0.3% traffic loss observed During Inservice NEF1 upgrade from 23.2.0 to 23.3.0	During in-service NEF1 upgrade from 23.2.0 to 23.3.0, 0.3% loss in traffic was observed.	3	23.3.0
35642697	NEF -TLS :GR setup : During Uninstall config-server and ocnef-expiry-auditor post delete hooks are not deleting properly	While uninstalling config-server and ocnef-expiry-auditor, the post delete hooks were not completely deleted.	3	23.2.0
35322961	TI Notification : For UP_PATH Change event DNAI Change type allowing EARLY_LATE both event at a time.	For UP_PATH change event, DNAI change type is allowing both EARLY_LATE events at the same time.	3	23.1.0
34995647	NEF is not sending notification to AF for the subscribed events (service_api_available/unavailable)	It was observed that NEF was not sending notification to AF for the `service_api_available` and `service_api_unavailable` subscribed events.	3	22.4.0
36424033	23.4.0 yaml file "configMapReloadEnabled: false" yaml file need to be provided to avoid the loss during upgrade.	During upgrade, the updated `oc-nef-custom-values_23.4.0 yaml file` where `configMapReloadEnabled` is set to false was required to avoid traffic loss.	4	24.1.0

Table 4-11 (Cont.) NEF 24.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36407575	Upgrade from 23.4.0 to 24.1.0 rc-4 is unsuccessful and Bug detected in charts	It was observed that upgrade from 23.4.0 to 24.1.0 was failing and multiple bugs were detected in charts.	4	23.4.0
34933822	Continuously error OCNEF-CAPIF-ERR-400-1005 observed on occapif-eventmgr logs.	In occapif-eventmgr logs, there were continuous OCNEF-CAPIF-ERR-400-1005 errors observed.	4	22.4.0
35398955	0.5% loss is observed while restoring the site after failover for 1hr	While restoring the site after failover for one hour, some traffic loss was observed.	4	23.1.2
35872872	In failover/restore scenario, after restoration we observe couple of restarts in mysqld pods on both sites in GR setup	After restoration, it was observed that mysqld POD restarts on both sites in GR setup.	4	23.3.0
36020164	CAPIF Installation show warnings in version 23.2.0	While installing CAPIF version 23.3.0, multiple warnings were displayed.	4	23.2.0
36112928	Model A,B,D ME-SCEF+NEF TC from regression is failing	For ME - SCEF+NEF Model A, B, and D cases, regression failure was observed.	4	22.4.0
36107847	Model-B ME-GMLC failover TC failing	For ME Location Reporting Model B, ATS TC failure was observed.	4	23.4.0
36129366	NEF-GR Site: 950tps mixed traffic: Replication break and recovered in few minutes (1 or 2 mins) After Rollback from 23.4.0 to 23.3.1 for CAPIF/NEF/CNDB both Site1 and Site2	Post roll back from 23.4.0 to 23.3.1, a replication break and recovery was observed.	4	23.4.0
36129191	Stubs are failing while Installation	During NEF 23.4.0 installation, it was observed that the stubs were failing to install.	4	23.4.0

Table 4-11 (Cont.) NEF 24.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36315560	Same alert "MENotificationFailure RateCrossedThreshold " is documented multiple times in the user guide	It was observed that there were multiple occurences of `MENotificationFailureRateCrossedThreshold` alert tables in the Oracle Communications Cloud Native Core, Network Exposure Function User Guide.	4	23.4.0
36276005	"ueIdentity" information is not sending correctly during ME update procedure towards UDM	During Monitoring Event update towards UDM, the ueIdentity information was not being sent correctly.	4	23.4.0

> **Note:**
>
> Resolved bugs from 23.4.2 have been forward ported to Release 24.1.0.

4.2.6 NRF Resolved Bugs

Release 24.1.3

NRF 24.1.3 Resolved Bugs

There are no resolved bugs in this release.

Table 4-12 NRF ATS 24.1.3 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37065026	NRF ATS 24.1.2 - Random regression test case failures	While doing full regression testing, random features failed while verifying the responses received from `slfOptions`.	3	24.1.2
37039789	NRF ATS 23.4.2 - populateSlfCandidateList did not return back to false	The value of `populateSlfCandidateList` did not change to default value (false), which resulted in failure of SLF test cases.	3	23.4.2

Release 24.1.2

Table 4-13 NRF 24.1.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
36941582	NRF Discovery requests failure after NRF upgrade to 23.4.2	When a discovery query was sent to CDS for retrieving the NFProfiles from the database, the database flushed out all the profiles from its in-memory cache due to an exception.	1	23.4.2
37026879	target-plmn-list query parameters when acting as vNRF	As per 3GPP, for NFDiscover service operation, it was not clear that NRF shall encode the array of objects query attributes as array exploded way or not. When the value of `exploded` was true, NRF followed exploded way of array which meant key-value pair and repeated the same attribute for each element of array. But some operators were following the non-exploded (value of `exploded` is set as false) form of the array. It meant the array of objects needs to be encoded as an array. This is applicable to NRF forwarding and NRF roaming cases.	3	23.4.0
37027034	Requester-snssais field misspelled in URL encoding during fowarding/roaming	The `requester-snssais` discovery query attribute was misspelled in URL encoding during forwarding and roaming scenarios.	3	24.1.1
37027561	After NRF upgrade to 23.4.2 aud claim in oauth token is causing 401 UNAUTHORIZED failures	After NRF upgrade to 23.4.2 ,`aud claim` in oAuth token was causing 401 UNAUTHORIZED failures. These failures occurred as third party library changed its behaviour by sending `aud` attribute in AccessTokenClaims as arrayed for NFType value instead of a string type value.	3	23.4.2
37027594	UAH propagation is happening for SLF queries	NRF propagated the User-Agent Header received in the discovery request via SCP/curl command for SLF queries.	3	23.3.0

Table 4-13 (Cont.) NRF 24.1.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37027629	NRF-discovery sending incorrect response with EmptyList nf profiles when nfServiceStatus is SUSPENDED	During the processing of `NFDiscover` service operation, when emptyList feature was enabled, NRF was not sending NFProfiles, where both `NFProfileStaus` and `NFServiceStatus` were SUSPENDED.	3	22.4.0
37027644	OcnrfTotalNFsRegisteredBelowCriticalThreshold alert is getting raised despite NFs are registered	Non Leader Auditor Pod doesn't peg the metric. Instead, it raised the value as 0 which met the condition for raising the alert.	3	23.2.2
37027659	oauth2 is missing correspondence between targetNfType:5G_EIR and serviceName n5g-eir-eic	AccessToken scope validation failed to accept the requests having `targetNfType` with underscore in the name and corresponding service names with a hyphen in the name.	3	23.4.1
37027664	OcnrfReplicationStatusMonitoringInactive alert is incorrectly getting raised.	Metric `ocnrf-replication-status-check` was not getting pegged when the flag `overrideReplicationCheck` was set to true. This raised a false alert.	3	24.1.0
37027651	NRF- Metric populated with method,dbOperation out of Possible values given for "ocnrf_dbmetrics_total" for feature - NRF Growth	"`ocnrf_dbmetrics_total`" metric populated the `method` and `dbOperation` dimensions with incorrect values whereas these dimensions should be mapped with the correct values.	4	23.4.0

Release 24.1.1

Table 4-14 NRF 24.1.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
36528244	Overload and pod-protection feature became disabled at Ingress Gateway and its corresponding configuration was reset when NRF 24.1.0 was installed from restored DBs with fault recovery as true.	Overload and pod protection feature was disabled at Ingress Gateway and its corresponding configuration was reset when NRF 24.1.0 was installed from restored database with fault recovery as true.	2	24.1.0
36377429	ocnrf-nrfconfiguration restarts during upgrade/install intermittently	ocnrf-nrfconfiguration restarted intermittently during upgrade/ installation.	3	24.1.0
36547680	NfStatusSubscribe had high latency when subscriptionLimit feature was enabled	NfStatusSubscribe had high latency when subscriptionLimit feature was enabled.	3	24.1.0

Table 4-14 (Cont.) NRF 24.1.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
36579599	NRF ATS 24.1.0- Jenkins TC Failures and GUI Feature Selection Issue	While testing NRF ATS 24.1.0, new feature, and regression test cases were failing in Jenkins. Additionally, in the ATS GUI, the option to select a single feature in both 'New Features' and 'Regression' was not available.	3	24.1.0

Release 24.1.0

Table 4-15 NRF 24.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
36129247	NRF 24.1.0: CNDB upgrade failing from 23.3.x to 23.4.0 due to invalid format of CNDB 23.4.0 custom-yaml.	Parsing issues in CNDB 23.4.0 custom-yaml were fixed as CNDB upgrade failed from 23.3.x to 23.4.0.	2	23.4.0
36199161	NRF 24.1.0: NRF23.2.0 SCP monitoring via SCP Health APIs Fails on HTTPS - ERROR Exception frame_size_error/ invalid_frame_length	SCP monitoring using SCP Health APIs failed on HTTPS with the ERROR Exception frame_size_error/ invalid_frame_length.	2	23.2.0
36209326	NRF 24.1.0: During NRF performance of 46.5K TPS, multiple restarts are observed in NRF EGW with CrashLoopBackOff.	During NRF performance of 46.5K TPS, multiple restarts were observed in NRF Egress Gateway with CrashLoopBackOff.	2	23.4.0
36263380	NRF 23.4.0 jaeger-agent No Longer Populates Jaeger; jaeger-collector Provides Only Incoming Request	Incorrect Jaeger values were mentioned in yaml files and documentation. The default value of Jaeger is updated.	2	23.4.0
36299325	NRF 24.1.0: NRF 23.4 No ALPN h2 in server Hello from NRF	NRF 23.4 does not return TLS Application Layer Protocol Negotiation (ALPN) extension from NRF IGW after NRF was upgraded from 23.2.0.	2	23.4.0
36274883	NRF IGW pods stuck in crashloopback during NRF upgrade	NRF Ingress Gateway pods got struck in crashloopback while performing the NRF upgrade.	2	23.4.0
36262758	NRF 24.1.0: NRF only consider a single plmn-id from nrfPlmnList to determine if a discovery request is inter-PLMN	NRF only considered a single plmn-id from nrfPlmnList to determine if a discovery request is inter-PLMN.	2	23.4.0
36321651	NRF 24.1.0: NRF marking AMF deregistered momentarily while there is no HB miss & no NfDegister request sent from AMF	NRF was marking AMF as deregistered momentarily while there was no heartbeat miss and no NfDegister request sent from AMF.	2	23.1.1

Table 4-15 (Cont.) NRF 24.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
36244350	NRF23.2.0 SCP monitoring via SCP Health APIs Fails on HTTP	NRF23.2.0 SCP monitoring using SCP Health APIs failed on HTTP.	2	23.2.0
36075578	NRF 24.1.0: NRF 23.2.0 returning 503 when microservice is in error state	NRF returned 503 error code in case of service failure instead of 500.	3	23.2.0
35330710	SLF-Discovery-Forwarding request is returning SLF_Not_Reachable response when the slfHost is not reachable and forwarded NRF response is empty.	NRF returned SLF based error rather response received from forwarded NRF	3	23.1.1
34986707	NRF 24.1.0: ocnrf_replication_status_check_total does not get scraped from the artisan pod	ocnrf_replication_status_check_total does not get scraped from the artisan pod.	3	22.3.2
36126390	NRF- any value (1,2,3,4,true) for "vsmfSupportInd" attribute in SmfInfo matches as true for feature - vsmf Support-ind in discovery	vSmfSupportInd attribute in smfInfo was accepting Integer value during Registration of profile and was converting it to true (for non-zero value) and false (for zero value).	3	23.4.0
36159057	NRF 24.1.0: Metrics are not pegging the right nfFqdn value	Certain metrics were showing the nfFqdn dimension value as "nfFqdn" instead of the actual nfFqdn value.	3	23.4.0
36213817	NRF User Guide - NF screening feature scope needs a modification	Documentation issue for NF Screening feature.	3	23.2.0
36234762	NRF 23.3.0 is getting upgraded successfully during post upgrade validation when table is missing or schema is incorrect for NfSubscription or NfRegistration Microservices.	NRF 23.3.0 was getting upgraded successfully during postupgrade validation when the table was missing or schema was incorrect for NfSubscription or NfRegistration Microservices.	3	23.3.0
36044187	NRF Installation is getting successful in Fault recovery scenario when NfInstances and NfSubscriptions tables are missing during post-Installation validation	NRF Installation got successful in Fault recovery scenario when NfInstances and NfSubscriptions tables were missing during post-Installation validation.	3	23.3.0
36375927	NRF is not updating NFServiceListMap in case priority is getting updated in NFService level during preferred locality features	NRF was not updated NFServiceListMap in case if priority was getting updated in NFService level during preferred locality features.	3	23.2.2
36244977	NRF-ATS 23.3.1 - Service Account creation issue for STUB installation in NRF-ATS 23.3.1	Service Account creation issue for STUB installation in NRF-ATS.	3	23.3.1

Table 4-15 (Cont.) NRF 24.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
36245620	Service Priority Updates for services for same service Name	Service Priority Updates for services for the same service Name when there was more than one service in NFProfile.	3	23.2.1
36157555	NRF 24.1.0: NRF- Incorrect NF Profiles (Suspended) in Discovery response when Registered NFProfile matches for feature - vsmf Support-ind in discovery	Suspended Profiles were sent as Registered (when the EmptyList feature was Enabled) in the Discovery Response when the Registered Profile met the condition "when vsmf-support-ind=true is not matching then Profile without vsmfSupportInd should be sent".	3	23.4.0
36249834	The sequence in which NF profiles are returned is inconsistent across one of the sites in NRF GR setup 23.4.0	The sequence in which NF profiles returned was inconsistent across one of the sites in NRF georedandant based deployment.	3	23.4.0
36245217	The total active registrations count is incorrect in NRF 23.4.0	The total active registrations count was incorrect in NRF.	3	23.4.0
36490644	AMF responding to NRF notification with 400 BAD Request due to operation in lower case	NRF is sending notificationData with profileChanges which contains op values in lower case. It shall be in upper case. Fix is done to send the op attribute in profileChanges as upper case.	3	23.4.0
36153971	Istio containers min CPU and Memory value for NRF IGW and EGW is incorrect in NRF Installation and Upgrade Guide	The Istio containers min CPU and Memory values for NRF Ingress Gateway and Egress Gateway were corrected in NRF Installation and Upgrade Guide.	4	23.4.0
36270004	Change the creating access token secret command	The secret creation command for the access token was updated.	4	23.4.0

Note:

Resolved bugs from 23.3.2 and 23.4.1 have been forward ported to Release 24.1.0.

4.2.7 NSSF Resolved Bugs

Release 24.1.1

Table 4-16 NSSF 24.1.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
36717719	NSSF 24.1.0 has error in TOSCA.meta file	The `TOSCA.meta` file was referenced `nrf` instead of `nssf`. Specifically, the `Entry-Definitions` field was incorrectly pointing to `Definitions/ocnrf_vnfd.yml` rather than the correct `./Definitions/ocnssf_vnfd.yml` file.	3	24.1.0
36670140	Internal: NSSF ATS 24.1.0, "Regression" pipeline test cases are failed	The following test cases were failing in the "Regression" pipeline in the lab setup: Subscription_Notification_Availability_Put negative_indirect_communication	3	24.1.0

Release 24.1.0

Table 4-17 NSSF 24.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
36228622	Files are missing in NSSF 23.4.0 installation package.	The directory structure did not match the format outlined in the "NSSF_Installation_Upgrade_and_Fault_Recovery_Guide," in section 2.2.1.2. Additionally, some files were also missing.	2	23.4.0
36373518	OCNSSF 23.4.0 is not providing "application_layer_protocol_negotiation (16)" ALPN TLS extension in Server Hello message	NSSF 23.4.0 was not providing the "application_layer_protocol_negotiation (16)" ALPN TLS extension in the Server Hello message.	2	23.4.0
36228208	NSSF ATS failure_methods feature is getting failed.	NSSF ATS failure_methods feature was getting failed.	3	23.4.0
36206925	NSSF ATS : Two feature files are not getting execute from ATS pipeline.	In the lab deployment of NSSF 23.4.0, the regression pipeline was initiated, but two feature files, named NsConfig_Put.feature and NsAvailability_Put_TacRange.feature, did not execute after starting the pipeline. Verification confirmed that both files were not blank.	3	23.4.0
36251935	In NSSF 23.4.0, Custom Values file mentions the incorrect algorithm "RSA256".	The `ocnssf_custom_values_23.4.0.yaml` included the incorrect algorithm "RSA256." It should be "RS256."	3	23.4.0

Table 4-17 (Cont.) NSSF 24.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
35927702	If TAC is already subscribed, and in Subscription-Patch request, the same TAC is added within TAIList, status code 422 is recieved which is not defined in yaml	If TAC was already subscribed and in the Subscription-Patch request, the same TAC was added within TAIList, the user received error code 422, which was not defined in the YAML configuration.	3	23.3.0
36097869	NSSF Should reject Patch request for adding TaiRangeList which is already subscribed.	NSSF should reject the Patch request for adding `TaiRangeList`, which is already subscribed. However, it was accepting the request.	3	23.4.0
35846922	Egress pod is not updating with the Entry done in DNS server "DNS SRV Based Selection of SCP in NSSF"	The Egress pod was not updating with the entry done in the DNS server "DNS SRV Based Selection of SCP in NSSF".	3	23.3.0
35794550	While sending Discovery Request NssfDiscovery sends Data:<Missing> paramater towards NssfEgw	During the transmission of a discovery request from NssfDiscoveryPod (10.233.114.198) to NssfEgw (10.233.104.248), an additional data packet containing a parameter "`Data:<Missing>`" was observed. This packet was not present during previous tests in version 23.1.0. As a result, the validation failed as the system was unable to recognize the unexpected packet.	3	23.3.0
35878635	2GR Setup: Replication Off; NSSF should send a 404 NOT FOUND for ns-availability delete request for site2 if ns-availability put request sent to site1	The expected response was for NSSF to reject the delete request for site2 due to replication being disabled, resulting in NSSF sending a "404 Not Found" message. However, a "204 No Content" response was received. In a separate attempt without the GR Setup, NSSF correctly returned a "404 NOT FOUND" message.	3	23.3.0
36312333	Key Validation of EnableEnhancedAllowedNSSAIComputation is missing in nssfsystemoption API.	If an incorrect key, such as "EableEnhancedAllowedNSSAIComputation" was used, NSSF did not validate the key and updated the value to null, which is incorrect behavior.	3	23.4.0
35638572	Discrepancy in statistics with NSSF 23.2 (Indirect communication)	The names of some metrics in the *Oracle Communications Cloud Native Core, Network Slice Selection Function User Guide* did not match with the ones found in Prometheus.	3	23.2.0

Table 4-17 (Cont.) NSSF 24.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
36263096	NSSF 23.4.0 Registration to NRF fails due to APP-INFO issue	NSSF registration to NRF was failing due to an issue with the app-info.	3	23.4.0
35986099	Memory threshold resource is not supported in the NSSF IGW pod protection feature. It should be included in the user guide.	*Oracle Communications Cloud Native Core, Network Slice Selection Function User Guide* should be updated with the information that memory threshold resource is not supported in the NSSF IGW pod protection feature.	3	23.3.0
36254254	23.4.0 NSSF Customer-Specific CSAR need new CV file with the resources included for hook jobs	The customer required a new NSSF `custom-values.yaml` file for version 23.4.0, including resources defined for hook jobs.	3	23.4.0
36278666	NSSF 23.2.0 Ingress & Egress Service down Alerts pop up in Prometheus	When both the Ingress and Egress services were up and running, the user was getting alerts that they were down.	3	23.2.0
35975916	User agent support for NSSF: NSSF is sending registration & heartbeat towards NRF with user agent when nfinstanceid is not present & addFqdnToHeader is true with proper fqdn value	NSSF was sending registration and heartbeat messages to NRF with a user agent when `nfinstanceid` was not present, and `addFqdnToHeader` was set to true with the proper FQDN value.	3	23.3.0
36119247	NSSF - NetworkPolicies from/to selectors are blocking the traffic	NSSF Network Policies coming from or directed to selectors were blocking the traffic.	3	23.2.0
36101350	NetworkPolicies on NSSF - Wrong ports for ingress-gateway filtering	For Network Policies on NSSF, the wrong ports were configured for ingress-gateway filtering.	3	23.3.1
36218686	NSSF Deployment has Default NodePort Assigned to NRF services.	After installing NSSF 23.2.0 CSAR, user identified that the NRF services "nrf-client-nfdiscovery" and "nrf-client-nfmanagement" were deployed with the NodePort service type. Due to security guidelines, the user needed to change the service type to ClusterIP, but the `custom-values.yaml` fiile did not provide an option to modify the service type for NRF services.	3	23.2.0

Table 4-17 (Cont.) NSSF 24.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
36075727	After configuring AMFSet, Subscription Request sent gives error code of 417	After configuring AMFSet, NSSF was expected to send discovery and subscription requests towards NRF, and successful configuration should have resulted in Discovery and Subscription Response as 201. Database analysis revealed that after AMFSet configuration, the `subscriptionId` for the configured AMF was initially NULL, updating after 10-15 seconds. This was not the case in the previous release, where the `subscriptionID` could be seen instantly after AMF configuration.	3	23.4.0
35690416	For the cpu usages indicator, NSSF is not raising the alert for OcnssfOverloadThresholdBreachedL1.	NSSF was not raising the alert for `OcnssfOverloadThresholdBreachedL1`.	3	23.2.0
35659396	NSSF must accept PATCH only when AMF also supports SUMOD	When “SUMOD” and “SupportedFeatureNegotiationEnable” were enabled in NSSF and the user executed the PATCH add operation after nssai-availability/subscriptions with POST message having supportedFeatures = “1”, that is AMF was not supporting SUMOD. Despite this, the PATCH add operation was happening successfully.	3	23.2.0
36323401	NSSF Network policy - Missing prometheus flow	When installing the NSSF default Network Policy, it blocked the communication between perf-info and Prometheus.	3	23.4.0
36430418	NSSF 23.4.0 ASM Installation Issue	The user attempted to install NSSF ASM and received an error. Also, the `custom-values.yaml` file provided with the NSSF ASM package had no support for multiple config key-value pairs.	3	23.4.0
36493445	AT NSSF ATS Ingress gateway Port is hardcoded to send messages to port 80	During NSSF015 ATS testing, an issue was faced with metrics test cases due to reliance on hardcoded Helm release names ""ocats"" and ""ocnssf"" for ATS and NSSF. To rectify this, modifications were required to eliminate dependence on hardcoded values, allowing flexibility in using relevant names for Helm releases across all components."	3	23.4.0

Table 4-17 (Cont.) NSSF 24.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
36488011	Metrics test cases encountered an issue related to naming problems with NSSF, ATS Helm release"	There were problems with the Regression and New Feature functionalities, likely due to issues with the configuration of the ingress port and Envoy filter. Additionally, there was a discrepancy between the ports used for exposing ingress-gw (8081) and the port configured for ATS to reach nssf-ingress-gw (80), leading to test case failures."	3	23.4.0
36520193	NSSF ATS 23.4.0 uses other PLMNs apart from 311 480 which leads to error response when supported PLMN list contaims only 311 480.	NSSF ATS 23.4.0 was using other PLMNs apart from 311 480, which led to an error response when the supported PLMN list contained only 311 480.	3	23.4.0
35966454	When AMF sends Patch request for adding a slice (EABB25) in subscribed TAC , I am recieving 2 notifications, one without slice EABB25 and then later one with the slice EABB25 in it.	When receiving a Patch request from AMF to add a slice (EABB25) in a subscribed TAC, two notifications were observed. The first notification did not include the slice EABB25, while the second notification, which was received later, included the slice EABB25.	4	23.3.0
36163812	Incorrect container Name in OcnssfPerfInfoService Down Alert Query	There was an issue with the `OcnssfPerfInfoServiceDown` Alert Query, where the container name was incorrect.	4	23.4.0
35701232	"422 Bad Request Error Json" even on not giving proper path value in PATCH request	On sending a PATCH request with an incomplete path request, 422 error code was coming but the error statement was not coming as "422 Bad Request Error Jason Patch Req processing failed".	4	23.2.0
36304751	NSSF 23.4.0 - Incorrect label value for performance POD	The performance pod had an incorrect label value assigned to it, showing as "pcf-perf-info" for NSSF 23.4.0 according to the pod description. It was recommended that the correct value should be either "perf-info" or "release-name-perf-info".	4	23.4.0

Table 4-17 (Cont.) NSSF 24.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
36167819	In Installation Guide 23.4.0, NSSF should remove the HELM possible value of podProtectionConfigMode.	In the *Oracle Communications Cloud Native Core, Network Slice Selection Function Installation, Upgrade, and Fault Recovery Guide* 23.4.0, the HELM option for pod protection was not supported. The Installation Guide incorrectly included HELM as an option for `podProtectionConfigMode`, while it should be only REST.	4	23.4.0
36169070	[Server header] Server header configuration sequence need to be updated in user guide NSSF 23.4.0	The configuration sequence for the Server Header was supposed to be updated in the *Oracle Communications Cloud Native Core, Network Slice Selection Function User Guide*.	4	23.4.0
35946049	"User Agent header" Mismatch in metric present in user guide and requirement page	The metrics in the *Oracle Communications Cloud Native Core, Network Slice Selection Function User Guide* related to the User Agent Header feature did not match with the ones in the Prometheus.	4	23.3.0
36225775	Load Metric for NF-Instance computation for the LCI header should be mentioned in the user manual.	The load metric for NF-Instance computation for the LCI header is determined by considering the average of the load metrics for both ns-selection and ns-availability. It was recommended to include this information in the *Oracle Communications Cloud Native Core, Network Slice Selection Function User Guide*.	4	23.4.0
35974141	"User agent header" : User guide need to be updated for Rest cmd.	URIs of some APIs in *Oracle Communications Cloud Native Core, Network Slice Selection Function REST API Guide* were incorrect.	4	23.3.0
36153873	Mention NSSF behaviour when serverheaderdetails & routesconfiguration configured without errorCodeSeriesId [Server Header]	When the configuration includes "serverheaderdetails" and "routesconfiguration" without specifying "errorCodeSeriesId" for the Server Header, the behavior of the NSSF (Network Slice Selection Function) in this context should be specified or addressed. It was recommended to clarify and document how NSSF responds or behaves under these conditions in the relevant documentation.	4	23.4.0

Table 4-17 (Cont.) NSSF 24.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
36088683	In Network Slice Selection Service, User guide states Requested NSSAI is mandatory paramater, whereas in 3gpp it is marked as Optional.	There was a discrepancy between the User Guide for the Network Slice Selection Service and the 3GPP specifications regarding the "Requested NSSAI" parameter. The *Oracle Communications Cloud Native Core, Network Slice Selection Function User Guide* indicated that the requested NSSAI is a mandatory parameter, while the 3GPP specifications mark it as optional.	4	23.4.0
35927764	If TAC 0 is subscribed then we send a patch request to add the same TAC, it accepts it. Multiple entries for TAC 0 is created in DB.	If TAC 0 was already subscribed, sending a patch request to add the same TAC resulted in acceptance. Consequently, multiple entries for TAC 0 were created in the database.	4	23.3.0

4.2.8 OCCM Resolved Bugs

Table 4-18 OCCM 24.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36246624	OCCM: With keyalgo as ECDSA, SECP256r1 option is missing in elliptic curve while creating x509 certificates	In the OCCM API and GUI, SECP256r1 was missing from the Elliptical Curve field and SECP256k1 was used instead.	3	23.4.0
36363889	OCCM 23.4.0: When requesting a NF certificate OCCM is sending IR with 2 SAN Extensions	OCCM included two SAN extensions in the IR while sending a request for an NF Certificate: • SAN extension with the DNA Name of the OCCM. • SAN extension with the relevant SAN of the NRF.	3	23.4.0
36368731	OCCM 23.4.0: DistinguishedName is not in valid format / C=FR/OU=XYZ/ CN=XYZ RA LTE OFR LAB - Bad Request	The user received the "DistinguishedName is not in valid format" error when they tried to use different formats for the Distinguished Name attribute to provision a user.	3	23.4.0

> **Note:**
>
> Resolved bugs from 23.4.1 and 23.4.2 have been forward ported to Release 24.1.0.

4.2.9 OCI Adaptor Resolved Bugs

Release 24.1.0

There are no resolved bugs in this release.

4.2.10 Policy Resolved Bugs

Table 4-19 Policy 24.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36125931	Every time RAR is triggered by PCF for Sd when SNR from OCS	For the same Charging Rule Base Name (CRBN), PCF by default was sending a RAR request toward Traffic Detection Function (TDF) on receiving the SNR message from OCS.	2	23.4.0
36149008	Binding Service throwing exceptions causing http2.remote_reset	Binding Service was throwing exceptions causing http2.remote_reset causing binding failure with BSF.	2	23.2.6
36224114	AMPCF 3gpp-sbi-target-apiroot incorrect.	In UE Service, when AMF discovery failed, then the default AMF API root configured for the simulator was used to send the subscriber request.	2	23.2.6

Table 4-19 (Cont.) Policy 24.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35406690	ASA logs have two response codes (5012 and 2001) but there is no 5012 in the metrics	When the PCRF service was sending an ASA, it was having two Diameter response codes (Diameter 5012 DIAMETER_UNABLE_TO_COMPLY and Diameter 2001 DIAMETER_SUCCESS). However, the 5012 code was not available in the metrics.	3	22.4.5
35996433	Diam-GW rejecting SLR even though the Discard Priority is set higher.	During Congestion Control testing, it was noticed that the Diameter Gateway was rejecting the SLR response even though the discard priority for Danger of Congestion (DOC) was set to the highest priority.	3	22.4.5
35524749	23.1.3 cnPCRF mismatched MIB information	The obsolete file imports were causing issues with mib validations resulting in mismatched MIB information for cnPCRF.	3	23.1.3
35939282	AM Session Delete 404 Error	AM-PCF successfuly created the AM Policy session. But few seconds later, it was observed that the AMF was sending delete request to AM-PCF, hence AM-PCF was responding with 404 Not Found Error.	3	23.2.2

Table 4-19 (Cont.) Policy 24.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36264911	RX and Binding sessions do not match	After enabling the Binding service (BSF), it was observed that the total number of RX sessions and the total number of Binding sessions did not match.	3	23.2.4
35870950	Issue with selecting correct CHF when PCF sending request to CHF	While attempting to retrieve the current NF instanceID during alternating routing, PCF consistently fetched the instanceID of the NF that was originally subscribed to, rather than fetching the instanceID of the currently failed NF.	3	23.2.2
36015501	NF Communication Profiles can not be created without 'Binding Level'	To enable the '3gpp-sbi-correlation-info' header, NF Communication Profile creation was done using the NF Correlation Settings of CNC Console. But PCF was not able to create the NF Communication Profile when the Binding level was set to empty. It was prompted to select either the NF set or the NF instance.	3	23.2.4
36220516	PCF does not re-evaluate policy during pending-tx	PCF was not re-evaluating policy during pending transaction.	3	23.2.4
36104991	User Service Replica Mismatch	User service was set to 20 replicas, but during upgrade, CHF unexpectedly scaled to 20 replicas, requiring manual scaling down to 4.	3	23.2.6

Table 4-19 (Cont.) Policy 24.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35998944	500 INTERNAL_SERVER_ERROR in PCFs for different messages in PCFs - AM and SM.	500 INTERNAL_SERVER_ERROR was observed in PCFs for different messages in PCFs- AM and SM.	3	23.2.4
36409994	Grant Quota Usage-Monitoring-Level --- PCC_Rule_Level	The functionality to grant quota with Usage-Monitoring-Level at PCC_RULE_LEVEL is not working as expected.	3	23.4.0
35990513	CNE 23.1.1 impact on PCF Service when restart One of the Master node	On restarting one of the Master Nodes, the PCF service was adversely affected, leading to a significant drop in total transactions per second from 5.16K to 100.	3	23.1.3
36034853	Policy Table "Matches" functionality not working as expected	Policy Table Matches functionality was not working as per the expectation.	3	23.2.5
36067751	cnPCRF 23.2.4 MatchList type String not matching whole item value	On using the blockly to compare a list with a matchList containing more than one element, it failed to perform the correct comparison.	3	23.2.4
36063694	N28 & N36 Delete after PRA IN transition from SM UPDATE	SM was triggering a CHF unsubs request right after receiving a response with absent SM/OSD Data from PDS.	3	23.2.6
35901207	cnPCRF 23.2.2 When Predefined PCC Rule Name does not match Rule Name, it doesn't get installed correctly	PCRF failed to install properly due to a mismatch between the predefined PCC Rule Name and the Rule Name.	3	23.2.2

Table 4-19 (Cont.) Policy 24.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35845050	PCF is not sending NCHF delete request	Following the successful termination of the N7 attach request, the PCF was supposed to send the NCHF delete request to CHF, yet the deletion request was not being sent as expected.	3	23.1.3
35524306	5G Production - Customer requesting alarmed for PCF Audit	An alert was required to be triggered for delete records in binding through audit, but the existing metrics related to audit was not sufficient to directly fetch the details.	3	23.1.5
35802731	Issue with PolicyDS-Request-Response PCF Dashboard (server_request_total) and (server_response_total)	There was an issue with PolicyDS-Request-Response in the PCF Dashboard for server_request_total and server_response_total KPIs.	3	22.3.4
35882628	PCF ingress gw logging warning for missing cm rss-ratelimit-map-kubernetes	The 'Rate-Limiting' parameter was disabled in the CNC Console but the 'missing cm rss-ratelimit-map-kubernetes' log messages were flooded in the NF logs.	3	23.2.2
36300230	Observing PCF Sending wrong Policy triggers during call Hold	PCF was sending wrong policy triggers during call hold operation.	4	23.4.0

Table 4-19 (Cont.) Policy 24.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36468286	SMservice Reject message with SESSION_NOT_AVAILABLE when request has framedip-IPv6	When Rx session with IPv6 and ipDomain was created, the look up for SM session takes both values to match and reject with session not found since SM session did not contain ipDomain.	4	23.2.1
36133039	CHF connector HTTP2 Remote Reset causing N28 create failure	CHF connector HTTP2 Remote Reset was causing N28 create failure.	4	23.2.6
34855425	PCF - Diameter gateway externalTrafficPolicy change query	A query was raised to modify "External Traffic Policy: Cluster" variable to "External Traffic Policy: Local" to avoid inter worker node communication.	4	22.3.0

Note:

Resolved bugs from 23.2.8 and 23.4.3 and have been forward ported to Release 24.1.0.

Table 4-20 Policy ATS 24.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
36334272	PCF_ATS Unexpected behaviour of service account in stub deployment	There was an unexpected creation of service accounts despite configuring the ServiceAccount.create parameters as false in the values.yaml file of ocstub-py.	4	23.4.0

4.2.11 SCP Resolved Bugs

Table 4-21 SCP 24.1.2 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37182465	SCP is not correctly applying the match filter when running the mediation traffic	The Mediation trigger point match criteria did not fail when headers defined were absent.	2	24.1.0
37182444	Mediation rule is not triggered when user-agent header	When Mediation rules were implemented and tested using the User-Agent header as a condition, the Mediation rules failed.	3	23.4.1
37182460	InterSCP Scenario - SCP sends invalid 3gpp-sbi-target-apiroot	The 3gpp-api-target-apiroot header was incorrectly populated for the inter-SCP scenario when the foreign producer profile did not have FQDN.	3	23.4.3
37182476	scp-worker not including query parameters when mediation rules is applied	SCP-Worker did not include query parameters when the Mediation rules were applied.	3	23.4.1
37182488	SCP Alternate Routing using DNS SRV not working	The SCP Alternate Routing using DNS SRV feature did not work.	3	23.4.1
37182490	Alternate Routing using Static Configuration not working as expected	The Alternate Routing using Static Configuration feature did not work.	3	23.4.0
37182511	SCP does not create routing rules for UDM	Routing rules were not created due to an exception in the RunQueueConsumer Thread.	3	23.2.2
37182517	scp-worker in crashloopbackoff when 2 out of 3 K8s master are down	SCP-Worker was crashing due to thread stuck when Kubernetes client was unavailable.	3	23.4.1
37088636	SCP not able to handle "invalidParams":null from BSF delete binding response	SCP was unable to handle "invalidParams":null from BSF delete binding response.	3	24.1.0
37049658	Unable to delete NFProfile via CNCC when Topology set to Local	Unable to delete NFProfile through CNC Console when the Topology_Source was set to Local.	3	24.1.0
36574593	Response headers when having 3gpp-sbi-target-apiroot doesn't follow IPv6 square bracket format	Response headers with 3gpp-sbi-target-apiroot headers did not follow the IPv6 square bracket format.	4	24.1.0

Note:

Resolved bugs from 23.3.0 have been forward ported to Release 24.1.2.

Table 4-22 SCP ATS 24.1.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36600481	ATS to consider IPFamilies as IPv4 by default when platform doesn't expose any ipFamilies	By default, ATS considered IpFamilies as IPv4 when the deployment did not expose any ipFamilies.	3	24.1.0

Table 4-23 SCP ATS 24.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36452116	23.4.1 ATS Regression Failure - SCP_Audit_nnrf_nfm_SMF_user_agent	In the ATS Console logs, remote_reset was observed while fetching the data from the nrf1. Therefore, the required messages were not captured that led to the test case failure at the validation step.	2	23.4.1
36352274	ModelC_CatchAll_Routing_Configuration_AUSF.feature failed	Metrics mismatch was observed for scenario 1 and scenario 2 of ModelC_CatchAll_Routing_Configuration_AUSF.feature while validating SCP 23.4.2 Regression features.	3	23.4.1
36600481	ATS to consider IPFamilies as IPv4 by default when platform doesn't expose any ipFamilies		3	24.1.0

Table 4-24 SCP 24.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36409549	SCP 23.4.1 : SNI not sent in TLS Handshake towards Producer NF	In SCP 23.4.1, SNI was not sent in TLS handshake towards Producer NF.	2	23.4.1
36338830	Configuration pod restart was noticed on SCP while configuring mediation rules	The SCP-Configuration pod restarted on SCP while configuring mediation rules.	2	23.4.0
36392964	SCP: TimeoutException:Timed out waiting for a node assignment resulting in back to back scp worker restarts	SCP: TimeoutException:Timed out waiting for a node assignment resulted in back to back SCP-Worker restart.	2	23.4.1
36270580	load manager, nrf-auth, and worker pods crashed while running the traffic with Model-D cache enabled as well as receiving an invalid response from NRF for nnrf-auth service	Load-manager, nrf-auth, and scp-worker pods crashed while running the traffic with Model-D cache enabled, and received an invalid response from NRF for nnrf-auth service.	2	23.4.0

Table 4-24 (Cont.) SCP 24.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36227588	Dashboards do not show data for model-C and model-D traffic	The SCP OCI dashboard did not show data for Model-C and Model-D traffic.	2	23.3.0
36211827	SCP's CPU utilization unexpectedly reached 80%, while its testing capacity and transaction pass rate decreased to 50%	SCP's CPU utilization unexpectedly reached 80% while its testing capacity and transaction pass rate decreased to 50%.	2	23.4.0
36386814	Routing Config Set on Console does not have an option to enable or disable the OCI feature for notification messages.	Routing Config Set on Console did not have an option to enable or disable the OCI feature for notification messages.	3	23.4.0
36377327	Implementation of 1st routing attempt and AR attempts on the basis of Interplmn FQDN or FQDN	Implementation of first routing and alternate routing were attempted on the basis of Interplmn FQDN or FQDN.	3	23.4.0
36377254	Same NF profile is picked up again and again for processing at notification as part of each and every audit cycle	The same NF profile was considered repeatedly for processing at notification as part of each audit cycle.	3	23.1.0
36325765	ocscp_audit_ondemand_success_total does not get incremented even when onDemand audit request, received with 2xx responses are invoked by scp	The `ocscp_audit_ondemand_success_total` metric was not incremented when SCP triggered onDemand requests. SCP received 2xx responses.	3	23.4.0
36316989	SCP returns an incorrect cause when a mandatory parameter in a Mediation Rule API request is missing	SCP returned incorrect cause when the mandatory parameter was missing in the Mediation Rule API request.	3	23.4.0
36340289	SCP 23.3.0 NF Profile Registration failed due to NF_RESOURCE_MAPPINGS table size	SCP 23.3.0 NF Profile registration failed due to NF_RESOURCE_MAPPINGS table size.	3	23.3.0
36341579	SCP does not permit changes to the code field and returns an error in the Applied state	SCP did not permit changes to the code field and returned an error in the applied state.	3	23.4.0
36353718	SCP returns response with body as unknown when target plmn list is not configured as a list	SCP returned response with body as unknown when the target PLMN list was not configured as a list.	3	23.4.0
36368930	service-instanceID is not getting generated for nnrf-oauth2 for dynamic NRF Profiles when NRF bootstrap info enabled	service-instanceID was not getting generated for nnrf-oauth2 for dynamic NRF Profiles when NRF bootstrap info was enabled.	3	23.4.0

Table 4-24 (Cont.) SCP 24.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36419216	Helm test validation needs to be corrected as the status shows succeeded even if mediation pod is not up	The Helm test validation was not corrected as the status showed "succeeded" even if the Mediation pod was not up.	3	23.2.0
36444487	Health check queries api-prefix needs to be validated with self api-prefix (scp-prefix) before accepting the request. If SCP does not have it configured that incoming health check request should also not have any api-prefix	SCP Health check queries api-prefix were validated with self api-prefix (scp-prefix) before accepting the request. If SCP did not have it configured, incoming health check request might not have any api-prefix.	3	23.4.1
36371943	ModelID enforceReqSpecificSvcDiscovery does not work with multiple service names coming in 3gpp-sbi-discovery-service-names	Model D `enforceReqSpecificSvcDiscovery` did not work with multiple service names available in 3gpp-sbi-discovery-service-names.	3	23.2.0
36302137	OCSCP Upgrade from 23.2.3 to 23.4.0 fails during e2eocscp2-scp-worker-post-upgrade job execution	SCP upgrade from 23.2.3 to 23.4.0 failed during e2eocscp2-scp-worker-post-upgrade job execution.	3	23.4.0
36297686	SCP doesn't clearly mention the duplicacy when there are duplicate nrf records on different SPNs in DNS SERVER	SCP did not mention the duplication when there were duplicate NRF records on different SPNs in the DNS server.	3	23.4.0
36262975	thread ID is not seen for the total number of response sent from SCP to Consumer NF	The thread ID was not observed for the total number of responses sent from SCP to consumer NF.	3	23.4.0
36255081	ocscp_configuration_dnssrv_nrf_non_migration_task_success_count_total counter is not getting pegged in case of TTL expiry modification from DNS server to SCP	The `ocscp_configuration_dnssrv_nrf_non_migration_task_success_count_total` counter did not peg in case of TTL expiry modification from DNS server to SCP.	3	23.4.0

Table 4-24 (Cont.) SCP 24.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36248672	SCP upgrade to 23.4.0 failing due to <.Values.sidecarPortExclusion.inBound>: nil pointer evaluating interface {}.inBound	SCP upgrade from 23.3.0 to 23.4.0 failed with the following error message: *Error: UPGRADE FAILED: template: ocscp/charts/scpc-alternate-resolution/templates/alternate-resolution.yaml:31:65: executing "ocscp/charts/scpc-alternate-resolution/templates/alternate-resolution.yaml" at <.Values.sidecarPortExclusion.inBound>: nil pointer evaluating interface {}.inBound.*	3	23.4.0
36222767	Validation of "deRegisterScpDuringMigration" parameter is missing for DNS SRV feature	The validation of the `deRegisterScpDuringMigration` parameter was missing for the DNS SRV feature.	3	23.4.0
36215062	metric to validate number of successful or failed deregistrations of SCP with NRF are missing	The metric to validate the number of successful or failed deregistrations of SCP with NRF was missing.	3	23.4.0
36163526	SCP responds to a request timeout for interPLMN with an incorrect body format.	SCP responded to a request timeout for InterPLMN with an incorrect body format.	3	23.4.0
36140430	SCP stop traffic after moving OCNADD-23.4.0 with 9094 to 9092 port	SCP stopped traffic after moving OCNADD-23.4.0 from 9094 to 9092 port.	3	23.4.0
36137584	SBA SCP23.2.0 Load Testing OCI Environment	When the load testing was performed using the PerfGO tool, the pod restarted at 99% of the load.	3	23.2.0
36096207	ocscp_worker_peer_oci_conveyance_total metrics shows incorrect ocscp_peer_nf_instance_id parameter value in case of InterPLMN	The `ocscp_worker_peer_oci_conveyance_total` metric displayed an incorrect `ocscp_peer_nf_instance_id` parameter value in case of InterPLMN.	3	23.4.0
36065896	SCP is indicating incorrect nf_type when alternate rerouting has made in an inter-plmn scenario	SCP indicated an incorrect nf_type when alternate rerouting was made in an inter-plmn scenario.	3	23.3.1
35988465	SCP respond with 503 error with invalid body in case of Oauth feature enabled	SCP responded with 503 error with invalid body when the OAuth feature was enabled.	3	23.3.0

Table 4-24 (Cont.) SCP 24.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35836629	Observed that 6.7 K 429's are generated due to PendingTransactionsPercentage overload in the run where there was no delay in response at producer with Oauth2 feature enabled	Users observed that 6.7 K 429's were generated due to PendingTransactionsPercentage overload in the run where there was no delay in response at producer NF with OAuth2 feature enabled.	3	23.3.0
36442059	Runtime state under feature status needs to be corrected in 24.1.0 User guide	Runtime state under feature status was supposed to be corrected in SCP 24.1.0 *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.	4	23.4.0
36442086	Possible values of runtime state under feature status section needs to be corrected in 24.1.0 User guide	Possible values of runtime stated under feature status section were supposed to be corrected in SCP 24.1.0 *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.	4	23.4.0
36486580	ocscp_nrfproxy_discovery_ondemand_discovery_response_cache_added_total metric names needs to be corrected in SCP User guide	The `ocscp_nrfproxy_discovery_ondemand_discovery_response_cache_added_total` metric name was incorrectly mentioned in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.	4	23.4.0
36376525	mandatory parameters for service level routing options is missing	The mandatory parameters for service level routing options were missing.	4	23.4.0
36332024	inconsistency in the user guide metrics	Users observed the following inconsistencies in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*: • For a few metrics, the ocscp_fqdn dimension was used instead of scp_fqdn. • In the ocscp_audit_tx_req_total metric, auditMode was mentioned as auditMod.	4	23.4.0

Table 4-24 (Cont.) SCP 24.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36321100	Missing description of LCI in Egress Congestion control feature	The Load Control Information (LCI) description was missing in the Egress Congestion Control feature section in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.	4	23.4.0
36316382	User Guide incorrectly mentions the default value and description of the maxRetryAttempts/ responseTimeout parameters	The default value and description of the `maxRetryAttempts/ responseTimeout` parameter was incorrectly documented in *Oracle Communications Cloud Native Core, Service Communication Proxy REST Specification Guide*.	4	23.4.0
36313438	User Guide's SCP Feature Status tab information is missing	The SCP Feature Status tab was missing from the *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.	4	23.4.0
36307160	User Guide's section on mediation rules needs to be updated	The Mediation Rules documentation was missing from *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.	4	23.4.0
36302749	supported values for multiple dimensions of ocscp_audit_rx_res_total and ocscp_audit_tx_req_total metric is missing in the user guide	The supported values for multiple dimensions of `ocscp_audit_rx_res_total` and `ocscp_audit_tx_req_total` metrics were missing from *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.	4	23.4.0
36301183	SCP is not specifying the error condition for number of failure attempts made while routing	SCP did not specify the error condition for the number of failure attempts made while routing.	4	23.4.0
36272832	SCP User Guide metrics corrections	Metric names were incorrectly documented in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.	4	23.4.0
36249895	Namespace names should to appear consistent across all panels on the default Grafana board.	The default Grafana dashboard did not display the namespace name consistently on each panel.	4	23.4.0

Table 4-24 (Cont.) SCP 24.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36248080	Possible values of the dimensions of DNS SRV feature metrics are missed in User guide of 23.4.0	The possible values of the dimensions of DNS SRV feature metrics were missing from SCP 23.4.0 *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.	4	23.4.0
36235505	pod name dimension mentioned incorrectly for scp metrics	The pod name dimensions were mentioned incorrectly for a few SCP metrics.	4	23.4.0
36225390	scp does not indicate the nrfSrvFqdn when it shows the status of DNSSRV NRF Migration task failure	SCP did not indicate the nrfSrvFqdn when it showed the status of DNSSRV NRF Migration task failure.	4	23.4.0
36216539	SCP Total Replicas (sum per hpa) displays an incorrect replica count In the default Grafana board	SCP Total Replicas (sum per hpa) displayed an incorrect replica count in the default Grafana board.	4	23.4.0
36168865	Metrics Title needs to be corrected in the metrics dashboard json file of 23.4.0 GA package	The metrics title required correction in the metrics dashboard `json` file of the SCP 23.4.0 GA package.	4	23.4.0
36048900	scp is not incrementing the alternate reroute metric when alternate producer is down	SCP did not increment the alternate reroute metric when alternate producer was down.	4	23.3.1

Note:

Resolved bugs from 23.2.0 have been forward ported to release 24.1.0.

Table 4-25 SCP ATS 24.1.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36600481	ATS to consider IPFamilies as IPv4 by default when platform doesn't expose any ipFamilies	By default, ATS considered IpFamilies as IPv4 when the deployment did not expose any ipFamilies.	3	24.1.0

Table 4-26 SCP ATS 24.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36452116	23.4.1 ATS Regression Failure - SCP_Audit_nnrf_nfm_SMF_user_agent	In the ATS Console logs, remote_reset was observed while fetching the data from the nrf1. Therefore, the required messages were not captured that led to the test case failure at the validation step.	2	23.4.1
36352274	ModelC_CatchAll_Routing_Configuration_AUSF.feature failed	Metrics mismatch was observed for scenario 1 and scenario 2 of ModelC_CatchAll_Routing_Configuration_AUSF.feature while validating SCP 23.4.2 Regression features.	3	23.4.1
36600481	ATS to consider IPFamilies as IPv4 by default when platform doesn't expose any ipFamilies		3	24.1.0

4.2.12 SEPP Resolved Bugs

Table 4-27 SEPP 24.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35916972	SEPP-PERF: n32-Egress-Gateway and PLMN-Ingress-Gateway pod restart due to OOMKilled (exit code 137) and 127 exit code and call failed observed with error code 503,504,408 & 500 during SEPP vanilla performance run at 62k MPS at SEPP_23.3.0	The overall system throughput has been reduced to 54K MPS with an increased pod count due to the Gateway restart issue. The per pod throughput was also reduced to 3200 MPS from 5000.	2	23.3.0
36323026	SEPP User Guide request to include [Metric] Type for all SEPP metrics defined, like all other NFs' User Guides	The metric type was not included in the metrics documentation of the *Oracle Communications Cloud Native Core, Security Edge Protection Proxy User Guide*.	2	23.4.0

Table 4-27 (Cont.) SEPP 24.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36373527	SEPP was not providing the "application_layer_protocol_negotiation (16)" ALPN TLS extension in the Server Hello message.	The ALPN extension was not sent in the server hello message of Igress Gateway when it acted as a server. Due to this, TLS traffic has been impacted in the case of different clients other than Egress Gateway and curl.	2	23.4.0
36324097	Error: Chart.yaml file is missing Raised when performing helm upgrade to apply network policies for SEPP	Due to the three-level directory structure in the tarball file: `ocsepp_csar / Files / Helm`, the automation script for dealing with SEPP charts failed before reaching the actual chart directory.	3	23.4.0
36285319	SEPP 23.2.0 | Network Policies Custom Values Needs Correction	In the metadata, the Ingress rule "allow-ingress-from-sepp-pods" allowed the traffic only from pods with "app.kubernetes.io/part-of: ocsepp", but the traffic from pods with "app.kubernetes.io/part-of: nrf-client" was also required. Due to this discrepancy, Egress traffic to the nrf-client pods was not allowed.	3	23.2.0
36239482	OCSEPP: Labels information missing in "SEPPCn32cHandshakeFailureAlert" raised on cSEPP and pSEPP	The container was missing in the labels for some of the alerts.	3	23.4.0
35890256	SEPP Helm chart does not pass Helm Strict Linting	SEPP Helm chart did not pass Helm Strict Linting.	3	22.3.2

Table 4-27 (Cont.) SEPP 24.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36285412	Network Policies Custom Values missing metadata "Allow egress to Prometheus"	The `ocsepp_network_policies_custom_values_23.2.0.yaml` file did not have the below metadata. *Allow egress to Prometheus-metadata:name: allow-egress-prometheus*	3	23.2.0
6142459	OCSEPP 23.4.0: SSL parameters need correction for GWs in 23.4.0 yaml	The description for the SSL parameters in custom-values and the Cloud Native Core, Security Edge Protection Proxy Installation, Upgrade, and Fault Recovery Guide was required to be updated.	3	23.4.0
34569424	Proper error-reason should be thrown by csepp when n32-ingress service is scaled down at psepp and an interplmn request is sent from csepp to psepp	The error scenario was observed when the Egress Gateway was not able to send the SBI message to the next node or NF when the NF was unreachable. The HTTP error status and the details in the response message received by the Egress gateway can be configured through the values.yaml file.error-reason:*org.springframework.web.reactive.function.client.WebClientRequestException:nested exception is java.nio.channels.ClosedChannelException*	3	22.2.0

Table 4-27 (Cont.) SEPP 24.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36026779	EGW restart observed	The Egress Gateway restart was observed at the capacity of 5000 MPS per POD, the issue requires more investigation and triage. As a temporary measure, the capacity was reduced to 3200 MPS per POD. The resource profile and dimensioning sheet have been updated to reflect this degradation.	3	23.3.0
36035492	PLMN IGW restarts due to java.lang.OutOfMemoryError	The Gateway restart was observed at the advertised capacity of 5000 MPS per POD and the PLMN Ingress gateway started showing out-of-memory issues, resulting in the restarting of the service. As a temporary measure, the capacity was reduced to 3200 MPS per POD. The resource profile and dimensioning sheet have been updated to reflect this degradation.	3	23.4.0
35750433	Incorrect deletion of action set and criteria set	The user was able to delete the action set and criteria set even though they are associated with routes.	3	23..4.0

Table 4-27 (Cont.) SEPP 24.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36071946	Mediation rule in draft state can be overwritten if user creates another mediation rule with same name	The mediation rule in the draft state could be overwritten if the user created another mediation rule with the same name. The user should not be able to overwrite the existing rule.	3	23.3.0
36293035	Initiate-On-Demand-Backup for single site NF shows 500 Error on GUI	Initiate-On-Demand-Backup for a single site NF was showing the error code 500 on GUI, but it was working fine when georedundancy was enabled on multiple sites.	3	23.4.0
36388875	RemoteSEPP config parameters are not aligned with REST document	The *Cloud Native Core, Security Edge Protection Proxy REST Specification Guide* has been updated with the following details of Remote SEPP parameter `isEnabled`: • default value of `isEnabled` = false	3	23.4.0

Table 4-27 (Cont.) SEPP 24.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36314126	Correct documentation for remotesepp config in rest guide.	In Remote SEPP REST API documentation, in the PUT method example, `seppFqdn` was set as IP, where IP was not being accepted.*"seppFqdn":"10.75.237.33","remoteSeppIpAddress":"10.233.62.145"*. In Remote SEPP REST API documentation, in "Sample response body structure for POST operations", the `remoteSeppIpAddress` was mentioned as "abc" whereas it should be valid IP.*"remoteSeppIpAddress":"abc"*	4	23.4.0
36253681	SEPP 23.4.0 CV Jaeger annotations update request	The unused variables were present in `ocsepp-custom-values-<version>.yaml` file. • `envJaegerAgentHost` • `envJaegerAgentPort`	4	23.4.0
35912471	For mediation, default error title should be configured	When a user was entering the error title at the Mediation -> Error configuration -> Title, with the feature set as false for the first time, the error title couldn't be saved until the user set the feature as true.	4	23.3.0

Table 4-27 (Cont.) SEPP 24.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36203736	OCSEPP: The InitialAlgorithm supported for each gateway should be mentioned in SEPP yaml	The comment section had to be updated to include details about the initial algorithm supported as ES256 and RS256.	4	23.4.0
36428222	dimensions are not matching for security_cert_x509_expiration_seconds metric	The metrics section in *Cloud Native Core, Security Edge Protection Proxy User Guide* has been updated with the dimensions of `security_cert_x509_expiration_seconds` metric.	4	23.4.0
36368414	Creating RemoteSeppSet is allowed with only secondary or tertiary SEPP	The Cloud Native Core, Security Edge Protection Proxy REST Specification Guide has been updated with the details.	4	23.4.0
36317104	Undocumented attribute “priority” returned in remotesepp config	The *Cloud Native Core, Security Edge Protection Proxy REST Specification Guide* had to be updated about the paramater `"priority"`.	4	23.4.0x
36317433	Configuration of "nfFqdn" for ingress and egress containers at SEPP custom file yaml file fails-CONFIGMAP files are do not call for the right nfFqdn value	While changing the nfFqdn value for n32-ingress, plmn-ingress, n32-egress, and plmn-egress microservices in SEPP `ocsepp-custom-values-<version>.yaml` file, changes were not getting reflected.	4	23.3.0

Note:

Resolved bugs from 23.3.2 have been forward ported to Release 24.1.0.

4.2.13 UDR Resolved Bugs

Table 4-28 UDR 24.1.1 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36617874	PCF egress traffic failing after 23.4.2 Upgrade	NRF Client sent an empty data frame in addition to the GET request while sending a GET request towards Egress Gateway.	1	23.4.3
36684616	Post upgrade to 23.4.3, Policy Create, Policy Update and Policy Delete have error 403 Forbidden	After upgrading to PCF 23.4.3, Ingress Gateway experienced 403 errors (SM CREATE/ UPDATE/ DELETE).	2	23.2.12
36682966	EgressGW http2.remote_reset	"http2.remote_reset" was observed in Egress Gateway logs.	2	23.2.12
36660374	Egressgateway buffer memory leak issue and alert missing	Alert was missing when there was Egress Gateway buffer memory leak.	3	23.4.0

Table 4-29 UDR 24.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36376646	For N36 10KTPS observing Exception in Notify service as mentioned below	During N36 10K TPS performance run, there was exceptions in notify service and drservice.	3	23.4.0
36265299	customAllowedUsage schema shall allow Negative value	The `customAllowedUsage` schema attribute was not allowing negative values.	3	23.4.0
36257397	EIR 23.2.0 : Format of the log file is not compliant to customer's request	The format of the log file generated after Provisioning Database Application (PDBI) bulk import was not compliant with the customer requirement.	3	23.2.0
36251604	SLF- In error Response of incorrect api ,cause field gives different description.	The cause field for incorrect API in the error response was providing a different error response description.	3	23.4.0
36244263	SLF- For Error Code 415, cause field is missing.	The cause field was missing for error code 415.	3	23.4.0

Table 4-29 (Cont.) UDR 24.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36224001	4G policy data export - Unable to import the 4G policy data exml export file into cnUDR after ixml conversion using Update operation	Unable to import the 4G policy data exml export file into cnUDR after converting the exml export files into ixml using ocudr xmlconverter.	3	23.4.0
36185398	Export tool status displays incorrect information for Exported Subscriber Count	Subscriber export tool status in CNC Console was displaying incorrect exported subscriber count.	3	23.4.0
36183360	Unable to import the 4G policy data exml export file into cnUDR after ixml conversion	Unable to import the 4G policy data exml export file into cnUDR after converting the exml export files into ixml.	3	23.4.0
36168970	Data inconsistency observed in UDR DB conflict resolution for Subscriber Key and Profile Data	Inconsistent data was observed in UDR database conflict resolution for subscriber key and profile data.	3	23.4.0
36167441	SLF- In DBCR feature, we have observed that one of the exception was not getting cleared even after running the dbcr audtior service came up	The exception was not getting cleared in the database conflict resolution feature even after running the database conflict resolution auditor service.	3	23.4.0
36142184	UDR migration tool "delete 4g subscriber" flag not getting enabled even when value is set as "true" in custom yml	In the migration tool, the delete 4G subscriber parameter flag was not getting enabled when the value was set to true in the custom yaml file.	3	23.4.0
36123246	UDR exporting empty 4G Policy data files if newFilePerRangeEnabled flag set to true	UDR was exporting empty 4G policy data files if the `newFilePerRangeEnabled` parameter flag was set to true.	3	23.4.0

Table 4-29 (Cont.) UDR 24.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36113121	UDR migration tool key type is showing as msisdn even when value is set as imsi in the yml	The migration tool was installed with key type as International Mobile Subscriber Identity (IMSI) in the yaml file but on the CNC Console key type was shown as Mobile Station Integrated Services Digital Network (MSISDN).	3	23.4.0
36095041	UDR diamGateway Realm and Identity is not getting updated even different values are given at time of installation	When UDR was installed or upgraded, the default value of `diamGatewayRealm` and `diamGatewayIdentity` was not getting updated.	3	23.4.0
36086757	DB Auditor Service not cleaning the ID2TODATA$EX table exception in site2	The user data was incorrect when state entity was deleted using PATCH.	3	23.3.1
36072268	UserData is incorrect when state entity is deleted via PATCH in UDR	The user data was incorrect when state entity was deleted using PATCH.	3	23.4.0
36069475	DB Auditor Service not cleaning the PROFILE_DATA$EX table exception in site1	Database auditor service was not cleaning the "PROFILE_DATA$EX" exception in Site1.	3	23.3.1
36025776	Result log stats is incorrect for empty pdbi files	The result log was incorrect for Provisioning Database Application (PDBI) files.	3	23.3.1
36017643	UDR nudr signaling GET operation is failing with error 404 "Subscriber does not exist" even when data is migrated from 4g to 5g udr.	The nudr signaling GET operation was failing with error 404 "Subscriber does not exist" when the subscriber data was migrated from 4G UDR to 5G UDR.	3	23.3.1
35762491	Diameter Gateway metric validation for missing avp in SNA and PUA response is getting pegged twice	The metric validation on diameter gateway for missing Attribute Value Pair (AVP) was pegged twice.	3	23.3.0

Table 4-29 (Cont.) UDR 24.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36094553	Notifications are inconsistently failing to reach server from egressgateway once 503 response is received from the server	Notifications were inconsistently failing to reach server from Egress Gateway, when 503 response was received from the server.	3	23.4.0
36372425	UDR migration tool summary report logs printing "List of failed target UDR keys" even the user are successfully migrated to 5G UDR	The migration tool summary report logs were showing "List of failed target UDR keys" even when the users were successfully migrated to 5G UDR.	4	23.4.0
36251676	SLF- In SLFSucessTxnDefaultGroupIdRateAbove50Percent label namespace is not printing	The namespace label was missing in the `SLFSucessTxnDefaultGroupIdRateAbove50Percent` alert.	4	23.4.0
36208127	4G policy data export - Export Status shows wrong export state if deletefromPVC is set to true	The export status was showing wrong export state in the CNC Console when `deletefromPVC` parameter was set to true.	4	23.4.0
36134404	Exml export tool parameter name fixedDumpFileNamePrefix adds string in suffix	The `fixedDumpFileNamePrefix` parameter value of the subscriber export tool was getting added into the suffix of exported dump.	4	23.4.0
36125609	QuotaTYPE table creation is not required for SLF/EIR upgrade to 23.4.0	To upgarde SLF or EIR to 23.4.0 release, creating QuotaTYPE table was not required.	4	23.4.0
36075847	201 Success message is missing for POST request in subscriber trace	POST request in the subscriber trace was missing 201 success message.	4	23.4.0

Note:

Resolved bugs from 23.3.2 have been forward ported to Release 24.1.0.

4.2.14 Common Services Resolved Bugs

4.2.14.1 ATS Resolved Bugs

Table 4-30 ATS 24.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36226485	Timeouts observed with 23.3.2 when sending higher traffic. Same is working fine with 23.3.1	Timeouts were observed with version 23.3.2 when handling higher traffic, while the same functionality worked fine with version 23.3.1.	2	23.3.0
36276138	Default Role and RoleBinding are getting created for the stub deployment even when a custom serviceAccount is mentioned in the custom values	Default role and role-binding were created for the stub deployment even when a custom service account was specified in the custom values.	2	23.3.2
35682371	Pystub: HTTP2 connection for get_all_payload API getting StreamReset Exception	The HTTP2 connection for the get_all_payload API received a StreamReset exception.	2	23.3.0

Note:

Resolved bugs from 23.3.2 have been forward ported to Release 24.1.0.

4.2.14.2 Alternate Route Service Resolved Bugs

Table 4-31 Alternate Route Service 24.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35964355	Alternate Route service not coming up when appinfoService is disabled	Alternate Route service was unavailable when `appinfoService` was disabled.	3	23.4.0

Note:

Resolved bugs from 23.4.0 have been forward ported to Release 24.1.0

4.2.14.3 Egress Gateway Resolved Bugs

Table 4-32 Egress Gateway 24.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36297302	OCBSF 23.4.0 is not providing "application_layer_protocol_negotiation (16)" ALPN TLS extension in Server Hello message	OCBSF 23.4.0 did not provide "application_layer_protocol_negotiation (16)" ALPN TLS extension in the Server Hello message.	2	23.4.3
36122972	List of Common Services screens not working correctly(EGW & IGW)	The list of Common Services screens did not work in Egress Gateway and Ingress Gateway.	3	23.4.0
36209140	Upgrade failure while converting Helm configuration to Rest configuration at PLMN EGW	Upgrade failed while converting Helm configuration to Rest configuration at PLMN Egress Gateway.	3	23.4.0
36253293	API-EGW and API-IGW Faulty metric regarding TLS Certificates (oc_certificatemanagement_tls_certificate_info)	API Egress Gateway and API Ingress Gateway used the faulty metric oc_certificatemanagement_tls_certificate_info regarding TLS certificates.	3	23.4.0
35463752	Multiple user agent headers are generated by Policy_EGW 23.1.4 during SM Create request to UDR	Multiple User-Agent headers were generated by Policy_EGW 23.1.4 during SM Create request to UDR.	3	23.1.4

Note:

Resolved bugs from 23.4.0 have been forward ported to Release 24.1.0.

4.2.14.4 Ingress Gateway Resolved Bugs

Table 4-33 Ingress Gateway 24.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
36297302	OCBSF 23.4.0 is not providing "application_layer_protocol_negotiation (16)" ALPN TLS extension in Server Hello message	OCBSF 23.4.0 did not provide application_layer_protocol_negotiation (16) ALPN TLS extension in the Server Hello message.	2	23.4.3
35722356	Getting intermittent BlackListIpException errors in one NEF microservice while inservice upgrade from 23.2.0 to 23.3.0	Received intermittent BlackListIpException errors in one of the NEF microservices while inservice upgrade was performed from 23.2.0 to 23.3.0.	3	23.3.1
36168856	IGW - RoutesConfigMode(REST) is not working	The `RoutesConfigMode` REST API did not work.	3	23.4.3
36326665	NRF 23.4.0 does not show any pending message count when IGW pod protection feature is enabled	NRF 23.4.0 did not show any pending message count when the Ingress Gateway pod protection feature was enabled.	3	23.4.3
35475399	REST API configuration of Pod protection feature is accepting requests without proper validation	The REST API configuration of the Pod Protection feature accepted requests without proper validation.	3	23.2.4
36261207	IGW JAVA errors observed after successful PCF deployment	Ingress Gateway JAVA errors were observed after deploying PCF.	3	23.4.3

Note:

Resolved bugs from 23.2.4 have been forward ported to Release 24.1.0.

4.2.14.5 Common Configuration Service Resolved Bugs

Table 4-34 Common Configuration Service 24.1.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36134944	SCP monitoring via SCP Health APIs Fails on HTTP	SCP monitoring through SCP Health APIs failed on HTTP.	2	23.2.4
36021839	"ConfigMaps watch closed" error occurring frequently on IGW	"ConfigMaps watch closed" error logs were observed on Ingress Gateway.	3	23.2.7

Note:

Resolved bugs from 23.2.4 have been forward ported to Release 24.1.0.

4.3 Known Bug List

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

4.3.1 BSF Known Bugs

Table 4-35 BSF 24.1.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36415688	BSF NetworkPolicy issue for egress flows	Default BSF Network Policy is blocking Egress Gateway call flows.	If BSF Network Policy is applied with the default rules, then the Egress traffic is blocked. **Workaround**: Remove deny-egress-all-except-egw network policy and add the appropriate allow/deny policy.	3	23.4.0

4.3.2 CNC Console Known Bugs

CNC Console 24.1.1

There are no known bugs in this release.

CNC Console 24.1.0

There are no known bugs in this release.

4.3.3 cnDBTier Known Bugs

cnDBTier Release 24.1.2

There are no new known bugs in this release. For the existing known bug, see "cnDBTier 24.1.1 Known Bugs".

cnDBTier Release 24.1.1

Table 4-36 cnDBTier 24.1.1 Known Bugs

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

cnDBTier Release 24.1.0

Table 4-37 cnDBTier 24.1.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36357037	Prod Db-tier Rolling restart stuck post Helm Upgrade for parameter change	cnDBTier rolling restart gets stuck post Helm upgrade when there is a parameter change.	`ndbmtd` pods get stuck post rolling restart of cnDBTier during the maintenance activity. Due to this georeplication is lost and the application traffic is impacted if it is not diverted before the maintenance activity starts. **Workaround:** • Scale down all the `ndbmtd` pods to zero and then scale them up. • Follow up with the georeplication recovery.	2	23.2.2
36234344	With BSF DB 23.2.2.0.0 upgrade, ndbmysqld all pods are restarting frequently	While performing a cnDBTier upgrade, all `ndbmysqld` pods restart frequently.	mysqld georeplication pods restart when they detect that the binlog injector thread is stalled. However, the automatic action results in a replication channel swicthover and georeplication continues. There is no impact to customer traffic due to the restart of mysqld georeplication. **Workaround:** The system performs the workaround automatically. The system restarts the mysqld geo replication pods when the code monitoring code detects that the bin log injector thread is stalled to prevent impact on the customer traffic.	2	23.2.2
36487409	dbtpasswd doesn't retain the old password in some of the pods	The `dbtpasswd` script doesn't retain the old password in some of the pods.	While using the `dbtpasswd` script, application pods with old password may not be able to connect to cnDBTier database. The connection of application pods depends on the mysqld pod that is used to attempt the connection with cnDBTier database. If the mysqld pod is one of the affected pods, then the connection fails. **Workaround:** Restart the application pods with the old passwords, so that the pods get the new password from Kubernetes secret.	3	23.4.2

4.3.4 CNE Known Bugs

Table 4-38 CNE 24.1.2 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
6740199	bmCNE installation on X9-2 servers fail	Preboot execution environment (PXE) booting occurs when installing Oracle Linux 9 (OL9) based BareMetal CNE on X9-2 servers. The OL9.x ISO UEK 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 4-38 (Cont.) CNE 24.1.2 Known Bugs

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

Table 4-39 CNE 24.1.1 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
6740199	bmCNE installation on X9-2 servers fail	Preboot execution environment (PXE) booting occurs when installing Oracle Linux 9 (OL9) based BareMetal CNE on X9-2 servers. The OL9.x ISO UEK 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 4-39 (Cont.) CNE 24.1.1 Known Bugs

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

CNE 24.1.0

There are no known bugs in this release.

OSO 24.1.0

There are no known bugs in this release.

4.3.5 NEF Known Bugs

NEF 24.1.0 Known Bugs

There are no known bugs in this release.

4.3.6 NRF Known Bugs

NRF 24.1.3 Known Bugs

There are no known bugs in this release.

NRF 24.1.2 Known Bugs

There are no known bugs in this release.

NRF 24.1.1 Known Bugs

There are no known bugs in this release.

Table 4-40 NRF 24.1.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36377429	ocnrf-nrfconfiguration restarts during upgrade/install intermittently	ocnrf-nrfconfiguration restarts during upgrade/ install intermittently. Pod comes to a normal state after a few seconds after some restarts.	There is no customer impact. **Workaround**: No workaround available	3	24.1.0
36318602	High rate of NfStatusNotify sent from NRF	Notifications are triggered from NRF when NFs move from one site to the other during some upgrade or maintenance.	High number of notifications are triggered from NRF when NFs move from one site to the other during some upgrade or maintenance. **Workaround**: There is no workaround but these scenarios are corner cases when some upgrade and maintenance activity is happening.	3	23.1.1

4.3.7 NSSF Known Bugs

Release 24.1.1

There are no new known bugs in this release. The known bugs from release 24.1.0 are also applicable to this release.

Release 24.1.0

Table 4-41 NSSF 24.1.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
36075599	Replication Channel has broken while doing CNDB rollback 23.4.0.rc.2 to 23.3.1 in site2	The Cloud Native Database (CNDB) utilizes a mechanism to replicate content across sites through binary log files (binlogs). Every database instruction executed at one Geographical Redundancy (GR) site is mirrored at the other. In specific scenarios, especially during rollbacks, replication performance may deteriorate under high transaction volume. Additionally, transaction ordering inconsistencies or omissions can occur, leading to potential constraint failures on the secondary site (for example, unique constraint violations due to missing deletes). Furthermore, any failure in binlog instructions disrupts the replication channel.	NSSF's Availability (NsAvailability) functionality may encounter a replication channel disruption when rolling back an upgrade from version 23.4.x to 23.3.x, especially if an availability delete and an availability update occur within a few seconds. **Workaround**: In the event of a broken replication channel, recovery can be initiated by following the procedures outlined in the *Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*. Refer to the section "Resolving	2	23.4.0

Table 4-41 (Cont.) NSSF 24.1.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
			Georeplication Failure Between cnDBTier Clusters in a Two Site Replication" in *Oracle Communications Cloud Native Core, Network Slice Selection Function Troubleshooting Guide* for detailed instructions on resolving the georeplication failure in a Cloud Native Core environment.		
36285762	After restarting the NSselection pod, NSSF is transmitting an inaccurate NF Level value to ZERO percentage.	Intermittently, NSSF displays a load of 0 during a restart scenario, but the condition returns to normal within a few minutes after the pod starts.	There is no impact on traffic. **Workaround**: No workaround available	3	23.4.0
36277930	If User-Agent Header is invalid, NSSF (HTTPS enabled) should not add the LCI and OCI Header.	In scenarios with HTTP enabled, NSSF provides a successful response with the calculation of the LCI/OCI header even when an invalid User Agent header is present.	There is no impact on traffic. **Workaround**: No workaround available	3	23.4.0

Table 4-41 (Cont.) NSSF 24.1.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36277891	If the Via Header is invalid, NSSF (HTTPS enabled) should not send the failure response.	When passing an invalid 'Via' header in a request with HTTPS enabled, a failure response is sent.	There is minimal impact on traffic. **Workaround**: No workaround available	3	23.4.0
36265745	NSSF is only sending NF-Instanse/NF-Service load level information for multiple AMF Get Requests	In a specific setup, NSSF intermittently sends only the instance load, even though the service-level load is also being calculated.	There is no impact on traffic. **Workaround**: No workaround available	3	23.4.0

Table 4-41 (Cont.) NSSF 24.1.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
36168261	NSSF does not discard packets as per the level configuration in ocdiscard policies.	NSSF is not consistently discarding the configured amount of traffic specified in discard policies when the error rate exceeds the threshold. When NSSF reaches a critical level based on the error rate, instead of rejecting 50%, it is rejecting 33.2%.	There is no impact on traffic. The reduction in discard percentage only occurs when the traffic contains errors exceeding 20%. Notably, this reduction does not have an impact on CPU usage, as observed during prolonged traffic runs where CPU levels remain stable. **Workaround**: The reduction in discard percentage occurs only when the traffic contains errors exceeding 20%. Notably, this reduction does not have an impact on CPU usage,	3	23.4.0

Table 4-41 (Cont.) NSSF 24.1.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
			as observed during prolonged traffic runs where the CPU remains stable.		
36158880	[Server Header] Patch operation is not working for errorcodeserieslist, Routeconfig & serverheaderdetails with NSSF 23.4.0	The patch operation for updating specific parameters in the error code series list, routes configuration, and server header details API occasionally malfunctions.	There is minimal to no impact on traffic. **Workaround**: In cases where the PATCH operation fails, the PUT operation can be employed with the complete configuration.	3	23.4.0

Table 4-41 (Cont.) NSSF 24.1.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
35975971	"User agent header support" NSSF is not adding User agent header in Registration, patch, Discovery & subscription towards NRF when "overwriteHeader :false" & in notification msg	NSSF fails to include the User Agent header despite the feature being enabled when the Override header is set to false towards NRF.	For call flows directed towards NRF, when the override header is set to false, the absence of the User Agent header is expected. This configuration does not directly impact the traffic. **Workaround**: Set the OverRide header as true.	3	23.3.0

Table 4-41 (Cont.) NSSF 24.1.0 Known Bugs

Bug Number	Title	Description	Customer Impact	SF Severity	Found in Release
35971708	while pod protection is disabled, OcnssfIngressGatewayPodResourceStateMajor alert is not clear and resource metric is not updating to -1	NSSF is unable to clear alerts when the pod protection feature is disabled.	There is no direct impact on traffic. However, when the pod protection feature is disabled, NSSF does not examine the state of the gateway pod, failing to clear associated metrics. **Workaround**: Once the pod protection feature is disabled, NSSF no longer examines the state of the gateway pod, resulting in the non-clearing of metrics. Check the resource state in Prometheus for further analysis.	3	23.3.0

Table 4-41 (Cont.) NSSF 24.1.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35962306	In a congested state, NSSF should reject a new incoming HTTP2 connection when AcceptIncomingConnections is set to false - Randomly Behaviour	NSSF is intermittently accepting connections in a congested state.	There is a chance of restarting if this behavior continues, but as per the testing, this is intermittent. **Workaround**: No workaround available	3	23.3.0
35922130	Key Validation is missing for IGW pod protection parameter name configuration	The Ingress Gateway (IGW) REST API configuration is missing validations for the Pod protection feature.	There is no impact as the operator can configure the system with appropriate values as outlined in the guide. **Workaround**: Configure NSSF with appropriate values as per *Oracle Communications Cloud Native Core, Network Slice Selection Function REST Specification Guide*.	3	23.3.0

Table 4-41 (Cont.) NSSF 24.1.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35921656	NSSF should validate the integer pod protection parameter limit.	The REST API for configuring pod protection lacks necessary validations.	`podprotection` configuration is accepting invalid values. **Workaround**: Configure NSSF with appropriate values as per *Oracle Communications Cloud Native Core, Network Slice Selection Function REST Specification Guide*.	3	23.3.0
35888411	Wrong peer health status is coming "DNS SRV Based Selection of SCP in NSSF"	NSSF fails to display an unhealthy status for a non-existent Service Communication Proxy (SCP).	There is no impact on traffic flow because a non-responsive SCP is not being considered for status, leading to the absence of any status indication. **Workaround**: No workaround available	3	23.3.0

Table 4-41 (Cont.) NSSF 24.1.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35860137	In Policy Mapping Configuration in Ingress Gateway, For the samplingPeriod parameter, max value of parameter validation should be necessary.	The REST API for configuring ocpolicymapping is lacking essential validations.	ocpolicymapping configuration is accepting invalid values.	3	23.3.0
35502848	Out of Range Values are being configured in PeerMonitoringConfiguration (Support for SCP Health API using HTTP2 OPTIONS)	The REST API for configuring `PeerMonitoringConfiguration` lacks necessary validations.	`PeerMonitoringConfiguration` is accepting an invalid value of timeout. **Workaround**: Configure NSSF with appropriate values as per *Oracle Communications Cloud Native Core, Network Slice Selection Function REST Specification Guide*.	3	23.2.0
36273800	NSSF 23.4.0 Jaeger integration issue	The Jaeger logs at NSSF could not be accessed.	There is no impact on traffic but there is an impact on debuggability. **Workaround**: No workaround available	3	23.4.0

Table 4-41 (Cont.) NSSF 24.1.0 Known Bugs

Bug Number	Title	Description	Customer Impact	SF Vulnerability Release
36372109	Rest API of NSSAI Auth for plmn, tac, tac range, and network slice are not updated for PUT Method and CNCC UI.	The REST API for configuring the `nssai_auth` Managed Object exhibits an issue where, while using the HTTP PUT method, only the Grant value is updated whereas the other parameters remain unaffected.	There is no impact on traffic. **Workaround**: Use DELETE and POST to update other parameters of `nssai_auth`.	24.1.0
35659396	When “SUMOD” & “SupportedFeatureNegotiationEnable” is enabled in NSSF and executing PATCH add operation after nssai-availability/subscriptions with POST message having supportedFeatures = “1” then also PATCH add operation is happening.	According to the NSSF specification, the HTTP PATCH method on subscriptions should only be allowed when the SUMOD feature is enabled. However, there is an issue as the NSSF currently permits the use of PATCH even when the feature is not enabled.	There is no impact on traffic as AMF on which SUMOD is not enabled does not try to send a PATCH. **Workaround**: No workaround available	23.2.0
36297806	NSSF is only sending NF-Instanse/NF-Service load level information for multiple AMF Get Requests	When multiple AMFs send requests to the `NsSelection` microservice, there is an inconsistency observed. For some requests, only NF-Instance scope LCI headers are received, while for others, only NF-Service scope LCI headers are present.	There is no impact on traffic. **Workaround**: No workaround available	23.4.0
36298095	After restarting the NSselection pod, NSSF is transmitting an inaccurate NF Level value to ZERO percentage.	Following the restart of the `NsSelection` pod, NSSF exhibits an issue wherein it transmits an inaccurate NF Level value.	There is no impact on traffic. **Workaround**: No workaround available	23.4.0

Table 4-41 (Cont.) NSSF 24.1.0 Known Bugs

Bug Number	Title	Description	Customer Impact	SF Vulnerability	Release
36326515	ocnssf-performance is not coming up and is throwing the error "Upgrade/rollback is in progress.	The `ocnssf-performance` pod fails to appear when performing multiple Helm upgrades to the same version.	There is no impact on traffic. **Workaround**: No workaround available		24.1.0
36372502	ocnssf-appinfo service is not displaying or editing in CNCC's Logging Level Options.	The `ocnssf-appinfo` service is experiencing an issue where it cannot be displayed or edited in CNC Console's Logging Level Options.	There is no impact on traffic. **Workaround**: No workaround available		24.1.0
36480323	At both sites, the error "Communications link failure" is displayed for every Ns-Selection pod logs.	The connection between NSSF and cnDBTier is breaking while running 5K traffic.	There is no impact on traffic. **Workaround**: It is a known issue in cnDBTier. No code fix is required. A troubleshooting procedure will be provided in NSSF documentation in upcoming release.		24.1.0

Table 4-41 (Cont.) NSSF 24.1.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35986361	NSSF will not modify the weight values in metrics simultaneously if the weight value changes. The weight metric has changed when any pod raises a new alarm.	NSSF, as part of pod protection, raises alerts when a pod is in a DOC (Deactivation of Communication) condition. The identified issue lies in the persistence of alerts. Once raised, the alert does not subside even after the condition is updated.	There is no impact on traffic as NSSF takes care of the condition but the alert is subsided only when there is a change in the state. **Workaround**: No workaround available	4	23.3.0
35855937	In Ingress Gateway's Error Code Series Configuration, The names of the exceptionList and errorCodeSeries parameters are not verified.	The REST API for configuring the error code series list lacks essential validations.	`errorcodeserieslist` is accepting invalid values. **Workaround**: Configure NSSF with proper values as per *Oracle Communications Cloud Native Core, Network Slice Selection Function REST Specification Guide*.	4	23.3.0

Table 4-41 (Cont.) NSSF 24.1.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35855745	Missing validation of the failureReqCountErrorCodeSeriesId mandatory parameter in the Ingress Gateway's Routes Configuration.	The REST API for configuruing `routesconfiguration` has missing validations.	`routesconfiguration` is accepting invalid values where the abatement value is less than the onset. **Workaround**: Configure NSSF with proper values as per Oracle Communications Cloud Native Core, Network Slice Selection Function REST Specification Guide.	4	23.3.0

Table 4-41 (Cont.) NSSF 24.1.0 Known Bugs

Bug Number	Title	Description	Customer Impact	SF Vulnerability	Release
35855377	The abatementValue less than onsetValue should be validated by NSSF in the Overload Level Threshold Configuration.	The REST API for configuring Overload Level Threshold Configuration has missing validations.	Overload Level Threshold configuration accepts invalid values where the abatement value is less than the onset. **Workaround**: Configure NSSF with proper values as per *Oracle Communications Cloud Native Core, Network Slice Selection Function REST Specification Guide*.	N	24.3.3.0
36271239	The ERROR message is being printed by NSSF for NF Scoring Calculation but NSSF is not supported the NF-Scoring feature	The `AppInfo` pod in NSSF is generating unnecessary error logs for an unsupported feature, leading to redundant error messaging.	There is no impact on traffic. **Workaround**: No workaround available	N	24.3.4.0
35845765	2-site GR setup ASM Enabled: During NSSF failover, IGW latency increased by 74 ms for ns-selection and 54 ms for ns-availability on site2	In failover scenarios, the observed latency exceeds 50 minutes, indicating a potential performance concern.	There is no impact on traffic. **Workaround**: No workaround available	N	24.3.3.0

Table 4-41 (Cont.) NSSF 24.1.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35796052	In Service Solution upgrade ASM enabled:2 Site GR Setup, Latency increases (237ms on site2 and 228ms on site2) observed during in service solution NSSF upgrade both sites from NSSF version 23.2.0 to 23.3.0	Intermittently, during in-service upgrade validation, latency exceeds the threshold of 50 minutes and reaches up to 237 minutes for certain messages. This variability in latency may raise concerns during the upgrade process.	There is no loss of service as this does not cause a timeout. **Workaround**: No workaround available	4	23.3.0
35297857	If AMF and NSSF enabled ONSSAI feature, NSSF should reject the ns-availability subscriptions request when taiList IE is non-empty array in ns-availability subscriptions request.	NSSF supports both the Tai List and Tai Range List; however, there is a discrepancy in the specification regarding whether both must be supported. As the support exists for both parameters separately and does not result in a loss of traffic, this issue is being maintained until further clarity is obtained from the specifications.	There is no impact on traffic. **Workaround**: No workaround available	4	23.1.0
36371261	AmfResolution data is not displayed uniformly in CNCC.	The CNCC GUI is currently not displaying all AMFs within an AMF set.	There is no impact on traffic. **Workaround**: No workaround available	4	24.1.0
35394240	CandidateAmfList is not added by NSSF when No AMF is sending the ns-availability update request to NSSF	None of the AMFs is sending the ns-availability update request to NSSF. The default PLMN, `plmnlevelnsiprofiles` has been configured by the operator. The operator configured `nss-rule` and `nssai-auth` for "EACA01" mapped to the default PLMN level profile. However, the AMF is not updating the ns-availability update request for the "EACA01" slice.	There is no impact on traffic. **Workaround**:	4	23.1.0

Table 4-41 (Cont.) NSSF 24.1.0 Known Bugs

Bug Number	Title	Description	Customer Impact	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.	In the specified scenario, with overload control initially enabled, the NSSF transitions into overload status, triggering an alert. Subsequently, when overload control is disabled, the alert fails to be cleared, contrary to the expected behavior where the alert should be removed upon disabling the feature.	There is no impact on traffic. **Workaround**: Enable the feature to clear the alert.	4	23.3.0

4.3.8 OCCM Known Bugs

OCCM 24.1.0 Known Bugs

There are no known bugs in this release.

4.3.9 OCI Adaptor Known Issue

OCI Adaptor 24.1.0 Known Issue

In this release, the Management Agent has a non-configurable scraping interval of 5 minutes. As a result, all the metrics get populated after 5 minutes. To change the value of scraping interval, see the "Troubleshooting Scenarios" section in the *Oracle Communications Cloud Native Core, OCI Adaptor Deployment Guide*.

4.3.10 Policy Known Bugs

Table 4-42 Policy 24.1.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36347854	extendedStackTrace being non-json format	Error log message observed in Binding pod logs, with extendedStackTrace which are considered to be in non-json format.	The PCF pod exceptions that contain *extendedStackTrace* are not parsing at Fluentd pods which results in missing messages in the Oracle CNE Kibana/ Opernsearch observability tools. **Workaround**: NA	3	23.2.4

Table 4-42 (Cont.) Policy 24.1.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release

36531557	Policy upgrade failing with "One of the Required Table is missing:eventssubscription" error in nwdaf agent	If upgrade is done after rollback, then it is failing with the "One of the Required Table is missing:eventssubscription" error in NWDAF agent.	This issue occurs when:
			• nwdaf-agent is enabled in the custom-values.yaml
			• Back to back upgrade: first upgrade to 24.1.0 and then rollback to the earlier release and finally upgrade again to 24.1.0.
			Upgrade fails in this case.
			Workaround:
			Workaround:
			1. Log into the ndbmysqld pod:
			`kubectl exec -it ndbmysqld-0 -n {namespace}- bash -c "mysql -u {user} -p {password} -h 127.0.0.1"`
			2. This these queries to verify the conflict_fn is on column UPDATED_TIMESTAMP:
			`use mysql; select CAST(db as char) as db, CAST(table_name as char) as tblName, CAST(conflict_fn AS CHAR) AS conflict_fn from ndb_replicatio`
				3	24.1.0

Table 4-42 (Cont.) Policy 24.1.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release

			`n where CAST(db as char) like "%nwdaf%";`
			3. Correct the column name in the conflict_fn by the query:
			`update ndb_replicatio n set conflict_fn='N DB$MAX_DEL_WIN _INS(updated_t imestamp)' where CAST(db as char) like "%nwdaf%";`
			4. Run the query again as mentioned in step 2 to verify that the column name is corrected.
			5. Recreate the table "eventssubscription" .		

36534793	"Timer Profile" Flag in Data Source Configurations need to be removed	The "Timer Profile" Flag in **Data Source Configuratio n** screen is not supported.	In data sources if the type is selected as "Sy", the timer profile will not have any impact in the call flow processing. **Workaround**: Do not use the timer profile if the type is selected as "Sy" in the **Data Source Configuration** Screen under **Create Data Source** on config-mgmt service in the CNC Console.	3	24.1.0

Table 4-42 (Cont.) Policy 24.1.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36539463	Search Criteria and Search Filter" Flags in Data Source Configurations are not unsupported and need to be removed	The "Search Criteria and Search Filter" flag in **Data Source Configuration** screen are not supported.	In data sources the Search Criteria and Search Filter will not have any impact in the call flow processing. **Workaround**: Do not use the Search Criteria and Search Filter in the **Data Source Configuration** Screen under **Create Data Source** on the config-mgmt service in the CNC Console.	3	24.1.0
36547814	When Bulwark/ Binding service is disabled from Custom yaml, after deploying Congestion Control setting on CM-UI becomes inaccessible	While installing PCF with disabled Binding/ Bulwark Service the Congestion Control Setting becomes inaccessible.	Do not use the Search Criteria and Search Filter in the Data Source Configuration Screen under Create Data Source on the config-mgmt service in the CNC Console. **Workaround**: Use swagger APIs to get/update Congestion Settings for services which are enabled.	3	24.1.0

4.3.11 SCP Known Bugs

SCP 24.1.2 Known Bugs

There are no known bugs in this release.

Table 4-43 SCP 24.1.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36451024	SCP Dashboard Does Not Display KPI data at Performance Level Traffic in OCI	SCP Oracle Cloud Infrastructure (OCI) dashboard does not display KPI data at performance level traffic in OCI.	A few widgets on the OCI dashboard might not be visible if a long interval is selected. **Workaround**: Add the "Error Messages for Mediation Rule Configuration" section in the *Oracle Communications Cloud Native Core, Service Communication Proxy Troubleshooting Guide* to describe how additional filters are added to reduce the number of samples of such KPIs.	2	24.1.0
36418752	SCP is not routing discovery to 2nd NRF After 1st NRF is shutdown	Stale destination entries in SCP routing rules are resulting in routing messages to the same NF repeatedly.	Message routing might happen to an already deregistered NF or the same NF multiple times. **Workaround**: Restart SCP-Worker to resolve the issue.	2	23.3.2

Table 4-43 (Cont.) SCP 24.1.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36526885	scp-worker not including query parameters when mediation rules is applied	SCP-Worker does not add query parameters when Mediation rules are applied.	The Mediation rule cannot be used to update any request with query parameters in the URI. **Workaround**: No workaround available	3	23.4.1
36526924	Metric "ocscp_interscp_health_check_status_failed" should be updated based on producer health status instead of traffic	The `ocscp_interscp_health_check_status_failed` metric should be updated based on the producer NF's health status instead of traffic.	The health status alert does not clear until the pod receives traffic for that NF. **Workaround**: It is an Info level alert. To clear the alert or update the alert file, send traffic to the producer NF.	3	23.4.1

4.3.12 SEPP Known Bugs

Table 4-44 SEPP 24.1.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
35036599	[SEPP-APIGW] Total traffic loss after upgrade when global Ingress rate limiting feature is enabled	The total traffic failure occurs when the SEPP is upgraded to 23.4.x and the rate limit feature is ON.The following exception occurs after the upgrade and also traffic is normal if the ingress pod is restarted.*Role=SpringframeworkBootLoaderJarLauncher))io.github.bucket4j.BucketConfiguration; class invalid fordeserialization"," message":"(Wrapped: Failed request execution forMapDistCache service on Member(Id=2*	If the Global RateLimiting feature is enabled with traffic in progress, and an upgrade is performed to any release, the upgrade n32-ingress-gateway stops processing traffic and there will be a total loss of traffic. **Workaround**: The following workarounds can be used: • If SBI traffic is in progress during the upgrade, restart the n32-ingress-gateway after the upgrade. The system will recover and start processing the traffic. • Perform an upgrade with theGlobal RateLimiting feature is disabled.	2	22.4.0

Table 4-44 (Cont.) SEPP 24.1.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
35527387	DNS SRV Support- Loss of SEPP forwarding Traffic at IGW with DNS SRV enabled at high TPS	The Egress Gateway restart is observed at the capacity of 5000 MPS per POD with the DNS SRV feature enabled.	The issue requires more investigation and triage. As a temporary measure, the capacity was reduced to 3200 MPS per POD. The resource profile and dimensioning sheet are updated to reflect this degradation. **Workaround**: No workaround available	3	23.2.3
35898970	DNS SRV Support- The time taken for cache update is not the same TTL value defined in SRV record.	The time taken to update the cache is not the same as the TTL defined in SRV records. Sometimes the cache updates even before TTL expires and at other times, the cache updates later than the TTL. Expectation: The cache must update once TTL has expired, hence if TTL is 60 then the cache must update after every 60s.	If the priority or weight is changed, it might take a longer time than TTL to get the cache updated and reflect the changes in the environment. **Workaround**: After changing the configuration, restart the `n32-egress-gateway` and `alternate-route-svc`.	3	24.1.0

Table 4-44 (Cont.) SEPP 24.1.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
35919133	DNS SRV Support-Custom values key "dnsSrvEnabled" does not function as described	In the custom values file, the *dnsSrvEnabled* flag is set to control considering if DNS-SRV queries are sent to coreDNS or not. If the flag is true, request should go to coreDNS, and if the flag is false, it must not go to coreDNS. However, when the flag is false and the setup is upgraded, the curl reaches core DNS.	In case of virtual FQDN, query will always go to core DNS. **Workaround**: Do not configure records in coreDNS	3	24.1.0
36111800	Generation of Watcher exception logs on IGW/EGW without any traffic	The Watcher exception logs are observed in gateway logs when SEPP is installed on the OCCNE 24.1.0-rc.1 cluster.	Extra error logs are observed which might result in filling ephemeral storage. **Workaround**: No workaround available	3	24.1.0
36209140	Upgrade failure while converting Helm configuration to Rest configuration at PLMN EGW	In the 24.1.0 release, the upgrade is successful. However, the Helm configurations are not converted to REST configurations. The entries for peer, peerset, and route configuration are not reflected in the common configuration table of the SEPP Database.	Already created Routes in Helm won't be converted to REST. **Workaround**: After performing an upgrade from Helm to REST, create the routes again through REST API.	3	23.4.0

Table 4-44 (Cont.) SEPP 24.1.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
36263009	PerfInfo calculates ambiguous values for CPU usage when multiple services are mapped to a single pod	In the `cgroup.json` file, multiple services are mapped to a single endpoint. The calculation of CPU usage is ambiguous. This impacts the overall load calculation.	The overall load calculation is not correct. **Workaround**: No workaround available	3	23.4.1
36266394	[OCI metric build] Load Metrics Query Interval Not Configurable	Load Metrics Query interval `prometheus_irate_range` is not Helm configurable. The default value is set to 2 minutes, which means that the rate calculation is normalized over samples within 2 minutes.	On changing the rate of traffic, it takes around 4 to 5 minutes to report the correct NF load to NRF. **Workaround**: Edit the perfinfo config map using `kubectl` command to change the `prometheus_irate_range` value.	3	23.4.1
36285390	oc_ingressgateway_global_ratelimit_total metric not pegging for Status "Dropped"	When the global rate limit is enabled on the ingress-gateway, for the metric `oc_ingressgateway_global_ratelimit_total`, the Status = "Dropped" label is not pegged. Only the "Accepted" status is pegged.	No alerts are raised for gateway for dropped messages. **Workaround**: No workaround available	3	23.3.2

Table 4-44 (Cont.) SEPP 24.1.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
34374452	SEPP-COM-xx-ERROR-0103 not observed when n32c pods have been scaled down	After scaling down pn32c and cn32c pods, if a delete request is run for configured Remote SEPP, the error code 204 is returned but the entry is not deleted.Also, no error is displayed when a POST request is run when the pods arescaled down.	There is no customer impact. Run the delete command when all the pods and services are Up and running. **Workaround**: The pod and service should be up and the commands will be run successfully.	4	22.3.0
35925855	x-reroute-attempt-count and x-retry-attempt-count header come twice in response when AR feature is enabled	Duplicate x-reroute-attempt-count and x-retry-attempt-count are observed	There is no customer impact. Duplicate headers are observed. **Workaround**: No workaround available	4	23.3.0

4.3.13 UDR Known Bugs

UDR 24.1.1 Known Bugs

There are no known bugs in this release.

Table 4-45 UDR 24.1.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36094811	Migration tool performance issue to read records from 4G UDR at high TPS	There is preformance issue from the migration tool to read records from 4G UDR at high TPS.	Migration time of data has increased. **Workaround**: No workaround available	3	23.4.0

Table 4-45 (Cont.) UDR 24.1.0 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36398645	UDR is sending Multiple Resources in notification for Subscriber deletion during Active Gx session	UDR was sending multiple resources in notification when subscriber was deleted during the active GX session.	It impacts only deletion of subscribers. **Workaround**: No workaround available	3	24.1.0
36424133	Unable to import the 4G policy data exml export file into cnUDR after ixml conversion with multiple msisdn keys	The exml export file into cnUDR couldn't be imported after converting the exml export files into ixml with multiple Mobile Station Integrated Services Digital Network (MSISDN) keys.	There is no customer impact. **Workaround**: The user can use two iXML to enable bulk provision of multiple keys.	3	24.1.0

4.3.14 Common Services Known Bugs

4.3.14.1 ATS Known Bugs

ATS 24.1.0 Known Bugs

There are no known bugs in this release.

4.3.14.2 Alternate Route Service Known Bugs

Alternate Route Service 24.1.0 Known Bugs

There are no known bugs in this release.

4.3.14.3 Egress Gateway Known Bugs

Egress Gateway 24.1.0 Known Bugs

There are no known bugs in this release.

4.3.14.4 Ingress Gateway Known Bugs

Ingress Gateway 24.1.0 Known Bugs

There are no known bugs in this release.

4.3.14.5 Common Configuration Service Known Bugs

Common Configuration Service 24.1.0 Known Bugs

There are no known bugs in this release.