Oracle® Communications

Cloud Native Core Release Notes

Release 3.25.1.100.0

G23953-10

August 2025

Oracle Communications Cloud Native Core Release Notes, Release 3.25.1.100.0

G23953-10

Contents

1 Introduction

2 Feature Descriptions

2.1 Automated Testing Suite (ATS) Framework 1
2.2 Binding Support Function (BSF) 1
2.3 Cloud Native Environment (CNE) 2
2.4 Cloud Native Core cnDBTier 5
2.5 Cloud Native Configuration Console (CNC Console) 8
2.6 Oracle Communications Cloud Native Core, Certificate Management (OCCM) 9
2.7 Network Repository Function (NRF) 10
2.8 Network Slice Selection Function (NSSF) 11
2.9 Service Communication Proxy (SCP) 12
2.10 Security Edge Protection Proxy (SEPP) 14
2.11 Unified Data Repository (UDR) 16

3 Media and Documentation

3.1 Media Pack 1
3.2 Compatibility Matrix 5
3.3 3GPP Compatibility Matrix 8
3.4 Common Microservices Load Lineup 9
3.5 Generic Open Source Software Compatibility on Any Platform 10
3.6 Security Certification Declaration 21
3.6.1 BSF Security Certification Declaration 21
3.6.2 CNC Console Security Certification Declaration 22
3.6.3 OCCM Security Certification Declaration 23
3.6.4 NRF Security Certification Declaration 24
3.6.5 NSSF Security Certification Declaration 25
3.6.6 SCP Security Certification Declaration 26
3.6.7 SEPP Security Certification Declaration 26
3.6.8 UDR Security Certification Declaration 29
3.7 Documentation Pack 29

4 Resolved and Known Bugs
4.1 Severity Definitions 1
4.2 Resolved Bug List 2
4.2.1 BSF Resolved Bugs 2
4.2.2 CNC Console Resolved Bugs 4
4.2.3 cnDBTier Resolved Bugs 8
4.2.4 CNE Resolved Bugs 28
4.2.5 NRF Resolved Bugs 34
4.2.6 NSSF Resolved Bugs 46
4.2.7 OCCM Resolved Bugs 52
4.2.8 SCP Resolved Bugs 53
4.2.9 SEPP Resolved Bugs 63
4.2.10 UDR Resolved Bugs 75
4.2.11 Common Services Resolved Bugs 78
4.2.11.1 ATS Resolved Bugs 78
4.2.11.2 ASM Configuration Resolved Bugs 78
4.2.11.3 Alternate Route Service Resolved Bugs 78
4.2.11.4 Egress Gateway Resolved Bugs 79
4.2.11.5 Ingress Gateway Resolved Bugs 82
4.2.11.6 Common Configuration Service Resolved Bugs 85
4.2.11.7 Helm Test Resolved Bugs 85
4.2.11.8 App-Info Resolved Bugs 86
4.2.11.9 Mediation Resolved Bugs 86
4.2.11.10 NRF-Client Resolved Bugs 86
4.2.11.11 Perf-Info Resolved Bugs 87
4.2.11.12 Debug Tool Resolved Bugs 87
4.3 Known Bug List 87
4.3.1 BSF Known Bugs 87
4.3.2 CNC Console Known Bugs 87
4.3.3 cnDBTier Known Bugs 88
4.3.4 CNE Known Bugs 91
4.3.5 NRF Known Bugs 102
4.3.6 NSSF Known Bugs 108
4.3.7 OCCM Known Bugs 117
4.3.8 SCP Known Bugs 118
4.3.9 SEPP Known Bugs 121
4.3.10 UDR Known Bugs 135
4.3.11 Common Services Known Bugs 136
4.3.11.1 ATS Known Bugs 136
4.3.11.2 ASM Configuration Known Bugs 136
4.3.11.3 Alternate Route Service Known Bugs 136

4.3.11.4 Egress Gateway Known Bugs 137
4.3.11.5 Ingress Gateway Known Bugs 139
4.3.11.6 Common Configuration Service Known Bugs 143
4.3.11.7 Helm Test Known Bugs 143
4.3.11.8 Mediation Known Bugs 143
4.3.11.9 NRF-Client Known Bugs 143
4.3.11.10 App-Info Known Bugs 143
4.3.11.11 Perf-Info Known Bugs 143
4.3.11.12 Debug Tool Known Bugs 143

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 3.25.1.100.0 - G23953-10, August 2025

cnDBTier 25.1.103 Release
Updated the following sections with the details of cnDBTier release 25.1.102:

- Media Pack
- Compatibility Matrix
- cnDBTier Resolved Bugs

SEPP 25.1.102 Release

Updated the following sections with the details of SEPP release 25.1.102:

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

Release 3.25.1.100.0 - G23953-08, July 2025

cnDBTier 25.1.102 Release

Updated the following sections with the details of cnDBTier release 25.1.102:

- Media Pack
- Compatibility Matrix
- cnDBTier Resolved Bugs

SEPP ATS 25.1.102 Release

Updated the following section with the details of SEPP ATS release 25.1.102:

- SEPP Resolved Bugs
- Media Pack

Release 3.25.1.100.0 - G23953-06, June 2025

CNE 25.1.101 Release

Updated the following sections with the details of CNE release 25.1.101:

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

OSO 25.1.103 Release

Updated the following sections with the details of OSO release 25.1.103:

- OSO

- Media Pack
- Compatibility Matrix
- OSO Resolved Bugs

SEPP 25.1.101 Release

Updated the following sections with the details of SEPP release 25.1.101:

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

Release 3.25.1.100.0 - G23953-05, June 2025

OSO 25.1.102 Release

Updated the following sections with the details of OSO release 25.1.102:

- Operations Services Overlay (OSO)
- Media Pack
- Compatibility Matrix
- OSO Resolved Bugs

CNC Console 25.1.100 Release

Updated the Media Pack details as upgrade from release 23.4.x is also supported.

Release 3.25.1.100.0 - G23953-04, May 2025

OSO 25.1.101 Release

Updated the following sections with the details of OSO release 25.1.101:

- Operations Services Overlay (OSO)
- Media Pack
- Compatibility Matrix
- OSO Resolved Bugs

CNC Console 25.1.100 Release

Updated the Media Pack details as upgrade from release 23.4.x is also supported.

Release 3.25.1.100.0 - G23953-03, May 2025

cnDBTier 25.1.101 Release

Updated the following sections with the details of cnDBTier release 25.1.101:

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

Release 3.25.1.100.0 - G23953-02, May 2025

Added a table in the following sections to list the license names for feature mapping:

- Binding Support Function (BSF)
- Cloud Native Environment (CNE)
- Cloud Native Core cnDBTier
- Cloud Native Configuration Console (CNC Console)
- Oracle Communications Cloud Native Core, Certificate Management (OCCM)
- Network Repository Function (NRF)
- Network Slice Selection Function (NSSF)
- Service Communication Proxy (SCP)
- Security Edge Protection Proxy (SEPP)
- Unified Data Repository (UDR)

Release 3.25.1.100.0 - G23953-01, April 2025

General Updates:

Added the following sections in Media and Documentation:

- Added the Generic Open Source Software Compatibility on Any Platform section to provide information about the open source software compatibility with CNC NFs.
- Added a table that lists the upgrade sequence for Cloud Native Core releases in the Media Pack section.
- Added a table that lists the CNE upgrade sequence in the Media Pack section.

BSF 25.1.100 Release

Updated the following sections with the details of BSF release 25.1.100:

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

cnDBTier 25.1.100 Release

Updated the following sections with the details of cnDBTier release 25.1.100:

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

CNC Console 25.1.100 Release

Updated the following sections with the details of CNC Console release 25.1.100:

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

CNE 25.1.100 Release

Updated the following sections with the details of CNE release 25.1.100:

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

NRF 25.1.100 Release

Updated the following sections with the details of NRF release 25.1.100:

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

NSSF 25.1.100 Release

Updated the following sections with the details of NSSF release 25.1.100:

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

OCCM 25.1.100 Release

Updated the following sections with the details of OCCM release 25.1.100:

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

SCP 25.1.100 Release

Updated the following sections with the details of SCP release 25.1.100:

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

SEPP 25.1.100 Release

Updated the following sections with the details of SEPP release 25.1.100:

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

UDR 25.1.100 Release

Updated the following sections with the details of UDR release 25.1.100:

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

- UDR Known Bugs

Common Services Resolved Bugs

- Egress Gateway Resolved Bugs
- Ingress Gateway Resolved Bugs
- Alternate Route Service Resolved Bugs
- Helm Test Resolved Bugs
- Mediation Resolved Bugs

Common Services Known Bugs

- Egress Gateway Known Bugs
- Ingress Gateway Known Bugs

1 Introduction

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

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

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

2

Feature Descriptions

This chapter provides a summary of new features and updates to the existing features for network functions released in Cloud Native Core release 3.25.1.1xx.0.

> **Note**
>
> CCNC-XXXX is an internal identification number of the feature.

2.1 Automated Testing Suite (ATS) Framework

Release 25.1.100

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

2.2 Binding Support Function (BSF)

Release 25.1.100

Oracle Communications Cloud Native Core, Binding Support Function (BSF) 25.1.100 includes the following enhancements:

- **Stale Binding Detection Audit, Report, and Recover**: Service disruptions caused by network storms, system overload, database latency, or other factors can interrupt signaling between the Policy and BSF, impacting session binding. BSF provides a mechanism to revalidate the binding information of a PDU session, and recover stale bindings, ensuring session integrity. For more information, see "*Stale Binding Detection Audit, Report, and Recover*" section in "*Oracle Communications Cloud Native Core, Binding Support Function User Guide*".
- **Stale Binding Manual Detection Tool**: Service disruptions caused by network storms, system overload, database latency, or other factors can interrupt signaling between Policy and BSF, impacting session binding. Currently, when binding is lost and Policy sessions are in a hung state, there is no way of knowing which sessions were lost or never received the binding. As a result, no action can be taken to solve this issue. The Binding Detection Tool addresses this by allowing manual queries of sessions created within a specific time frame in both Policy and BSF. For more information, see *Oracle Communications Cloud Native Core, Binding Detection Tool User Guide*.
- **Enhancements in menu.json for cnDBTier GRR Configuration**: The BSF CNC Console GUI supports integration of read-only Georeplicaiton Recovery (GRR) cnDBTier APIs. With this, users can have specific information on cnDBTier statuses on the CNC Console. For more information, see the "*Support for cnDBTier APIs in CNC Console*" section in *Oracle Communications Cloud Native Core, Binding Support Function User Guide*.
- **Performance enhancement to achieve 54K TPS**: In this release, BSF can achieve 54K TPS through performance optimizations. For more information, see the "*BSF Benchmark Testing*" section in *Oracle Communications Cloud Native Core, Binding Support Function Benchmarking Guide*.

- **Traffic Segregation**: BSF supports end-to-end traffic segregation based on traffic types. This ensures that critical networks are not cross-connected or share the same routes, thereby preventing network congestion. For more information, see the "*Traffic Segregation*" section in *Oracle Communications Cloud Native Core, Binding Support Function User Guide*.

The following table lists the license names for feature mapping. For additional licensing information, see *Oracle Communications Cloud Native Core Licensing Information User Manual*.

Table 2-1 License names for feature mapping

License Name	CCNC Number	Feature Name
Oracle Communications Cloud Native Core, Binding Support Function - 25K Active Subscribers Perpetual	CCNC-8864	Stale Binding Detection Audit, Report, and Recover
Oracle Communications Cloud Native Core, Binding Support Function - 25K Active Subscribers Perpetual	CCNC-8840	SMPCF and BSF Stale Binding Manual Detection Tool
Oracle Communications Cloud Native Core, Binding Support Function - 25K Active Subscribers Perpetual	CCNC-5795	Enhancements in menu.json for cnDBTier GRR Configuration
Oracle Communications Cloud Native Core, Binding Support Function - 25K Active Subscribers Perpetual	CCNC-7763	Compatibility with two Webscale versions per release
Oracle Communications Cloud Native Core, Binding Support Function - 25K Active Subscribers Perpetual	CCNC-4504	Performance enhancement to achieve 54K TPS
Oracle Communications Cloud Native Core, Advance Cloud Native Environment - 25K Active Subscribers perpetual	CCNC-4443	Traffic Segregation

2.3 Cloud Native Environment (CNE)

Release 25.1.101

Oracle Communications Cloud Native Core, Cloud Native Environment (CNE) 25.1.101 includes the following enhancement:

Support for Multus Thick Plugin for CNE deployments: With this feature, Multus Thick Plugin is installed whenever a new version of CNE is installed with CNLB enabled option. It is highly recommended to use Multus Thick Plugin based release for CNLB based CNE deployments. For more information, see *Oracle Communications Cloud Native Core, Cloud Native Environment User Guide.*

> **Note**
>
> - Only CNE Releases 24.3.3 and above support Multus Thick Plugin based CNE deployments.
> - CNE 24.2.x releases do not support Multus Thick Plugin and are not recommended for CNLB deployments.

Release 25.1.100

Oracle Communications Cloud Native Core, Cloud Native Environment (CNE) 25.1.100 includes the following enhancements:

- **Support for BareMetal CNE Deployment with Bare Minimum Servers (3 Worker Nodes)**: With this feature, CNE allows you to set up a BareMetal deployment with a minimal resources of three worker nodes. This setup is ideal for testing and getting started with CNE. For more information about installing and upgrading CNE with bare minimum servers, see the "*Installing CNE using Bare Minimum Servers*" and "*Upgrading BareMetal CNE Deployed using Bare Minimum Servers*" sections respectively in *Oracle Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide*.
- **Hardware Agnostic Deployment Model for BareMetal CNE**: Currently, CNE validates and supports BareMetal deployments on HP Gen10 and Oracle X8-2 servers only. With this release, CNE supports installing BareMetal CNE on any servers, thereby allowing the users to choose their servers based on their requirement. For more information about the prerequisites and updated procedure to install BareMetal CNE on other servers, see the "*BareMetal Installation*" section in *Oracle Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide*.
- **Heterogenous Hardware Support for BareMetal CNE Deployment**: Currently, BareMetal deployments support homogeneous hardware make, type, and version for worker nodes in a cluster. This means, all the worker nodes in a cluster must have the same type of hardware server, type, and version (for example, HP Gen 10 server with similar CPU, cores, RAM, and storage). With this feature, CNE supports heterogeneous hardware, wherein worker nodes in a cluster can have different server, type, and version. This provides more flexibility and options to manage hardware failure, expand existing deployment cluster, and tackle hardware End Of Life (EOL) and availability. For more information, see *Oracle Communications Cloud Native Core, Cloud Native Environment User Guide* and *Oracle Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide*.
- **Generic ToR Switch Configuration for BareMetal CNE**: With this feature, CNE facilitates you to set up your BareMetal cluster using any ToR switch, by providing generic specifications, prerequisites, and configuration templates. For more information about configuring the ToR switches, see the "*Configuring Top of Rack Switches*" section in *Oracle Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide*.
- **Traffic Segregation**: With this enhancement, CNE provides an option to use Cloud Native Load Balancer (CNLB) without internal traffic segregation. This means CNLB can be configured to have a single interface to handle only external traffic. For more information about CNLB configuration, see *Oracle Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide*.
- **New Versions of Common Services**: The following common services are upgraded in this release:

- Helm - 3.16.2
- Kubernetes - 1.31.1
- Calico - 3.28.0
- Istio - 1.23.0

To get the complete list of third-party services and their versions, refer to the `dependencies_25.1.100.tgz` file provided as part of the software delivery package.

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

The following table lists the license names for feature mapping. For additional licensing information, see *Oracle Communications Cloud Native Core Licensing Information User Manual*.

Table 2-2 License names for feature mapping

License Name	CCNC Number	Feature Name
Oracle Communications Cloud Native Core, Cloud Native Environment - per 25K Subscribers Perpetual	CCNC-6155	Support for BareMetal CNE Deployment with Bare Minimum Servers (3 Worker Nodes)
Oracle Communications Cloud Native Core, Cloud Native Environment - per 25K Subscribers Perpetual	CCNC-7674	Hardware Agnostic Deployment Model for BareMetal CNE
Oracle Communications Cloud Native Core, Cloud Native Environment - per 25K Subscribers Perpetual	CCNC-8297	Heterogenous Hardware Support for BareMetal CNE Deployment
Oracle Communications Cloud Native Core, Cloud Native Environment - per 25K Subscribers Perpetual	CCNC-7672	Generic ToR Switch Configuration for BareMetal CNE
Oracle Communications Cloud Native Core, Advanced Cloud Native Environment - 25K Active Subscribers Perpetual	CCNC-8079	Traffic Segregation
Oracle Communications Cloud Native Core, Advanced Cloud Native Environment - 25K Active Subscribers Perpetual	CCNC-1192	Multiple Network Interface per POD Support

Operations Services Overlay (OSO)

Release 25.1.103

Oracle Communications Cloud Native Core, Operations Services Overlay (OSO) 25.1.103 includes the following enhancements:

- **Support for new versions**:
  - `25_1_common_oso:25.1.103`

  - `25_1_oso_snapshot:25.1.103`

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

Release 25.1.102

Oracle Communications Cloud Native Core, Operations Services Overlay (OSO) 25.1.102 includes the following enhancements:
Support for new versions:

- `25_1_common_oso:25.1.102`
- `25_1_oso_snapshot:25.1.102`

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

Release 25.1.101

Oracle Communications Cloud Native Core, Operations Services Overlay (OSO) 25.1.101 includes the following enhancements:
Support for new versions:

- `25_1_common_oso:25.1.101`
- `25_1_oso_snapshot:25.1.101`

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

Release 25.1.100

Oracle Communications Cloud Native Core, Operations Services Overlay (OSO) 25.1.100 includes the following enhancements:

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

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

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

- **Support for new versions**:
  - `25_1_common_pod` is replaced with `25_1_common_oso`.
  - `25_1_oso_snapshot:25.1.100`

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

2.4 Cloud Native Core cnDBTier

Release 25.1.103

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

Release 25.1.102

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

Release 25.1.101

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

Release 25.1.100

Oracle Communications Cloud Native Core, cnDBTier (cnDBTier) 25.1.100 includes the following enhancements:

- **Enhanced Georeplication Recovery using Parallel Backup Transfer and Restore**: The backup transfer and restore mechanism used during a georeplication recovery involved additional data compression at the data node and serial backup transfer to the remote sites. This impacted the performance of georeplication recovery. With this feature, cnDBTier implements the following enhancements in backup transfer and restore thereby improving the performance and efficiency of georeplication recovery:
  - Avoids additional backup compression.
  - Supports parallel backup transfer from healthy cluster to georeplication recovery cluster.
  - Restores data node backups in parallel, as and when the backups are transferred from the healthy cluster to the georeplication recovery cluster.

  For more information, see *Oracle Communications Cloud Native Core, cnDBTier User Guide* and *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide.*
- **Support for TLS**: With this enhancement, cnDBTier supports TLS for application SQL pods to establish secure connection for communication with Network Functions (NFs). When the TLS feature is enabled, cnDBTier performs or supports the following operations during communication with NFs:
  - The application SQL pod uses the certificates provided or configured to establish an encrypted connection for communication with NFs. This encrypted connection remains throughout the life cycle of the connection between NF and cnDBTier.
  - The system reestablishes the TLS connection between NFs and cnDBTier after a georeplication recovery. That is, when a georeplication recovery completes successfully, the system reestablishes the encrypted connection between the NFs and cnDBTier. This ensures that cnDBTier continues supporting TLS connection after a georeplication recovery.

  For more information, see *Oracle Communications Cloud Native Core, cnDBTier User Guide* and *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide.*
- **Monitoring Cluster Events to Determine Data Loss in Clusters**: Network issues in the user environment led to cluster disconnections, which in turn resulted in the loss of cluster data. However, users were unable to monitor and identify the loss of data occurred due to network issues. With this feature, cnDBTier provides the following REST APIs to monitor cnDBTier cluster events to determine any data loss:
  - http://<base-uri>/db-tier/reset/parameter/cluster_restart_disconnect
  - http://<base-uri>/db-tier/reset/cluster/{cluster-name}/parameter/cluster_restart_disconnect

  - http://<base-uri>/db-tier/cluster/status
  - http://<base-uri>/db-tier/cluster/status/events/{numberOfLastEvents}
  - http://<base-uri>/db-tier/all/cluster/status/
  - http://<base-uri>/db-tier/all/cluster/status/events/{numberOfLastEvents}

  For more information about these APIs, see *Oracle Communications Cloud Native Core, cnDBTier User Guide.*

- **Storing NDB Logs in PVC**: cnDBTier stores all NDB pod (ndbmgmd, ndbmysqld, ndbappmysqld) logs in PVC. These logs remain persistent even when the pods restart and they can be used to debug any data node related issues. However, ndbmtd logs were not stored in PVC. With this feature, cnDBTier stored ndbmtd logs in PVC, such that the logs remain available even after the pod is deleted. This feature is enabled in cnDBTier by default and doesn't require any configuration. For more information, see the "*Storing NDB Logs in PVC*" section in *Oracle Communications Cloud Native Core, cnDBTier User Guide.*
- **cnDBTier Automated Backup**: MySQL doesn't allow schema change in a cluster when a backup is in progress. However, users were unable to check the ongoing backup processes in the cluster and schedule their upgrades for schema changes. With this release, cnDBTier provides the http://<base-uri>/db-tier/status/cluster/local/backup REST API to fetch the details of the data node backups that are in progress in the NDB cluster. For more information about this API, see the "*cnDBTier Backup APIs*" section in *Oracle Communications Cloud Native Core, cnDBTier User Guide.*
- **cnDBTier Scaling**: With this release, cnDBTier automates the vertical scaling of PVCs using the `dbtscale_vertical_pvc script`. This simplifies the vertical scaling process and reduces human errors that may occur while performing the manual procedure. For more information about performing the vertical scaling using the `dbtscale_vertical_pvc` script, see the "*cnDBTier Scaling*" section in *Oracle Communications Cloud Native Core, cnDBTier User Guide.*
- **Support for New Versions of Software**: cnDBTier has updated the version of Oracle MySQL Cluster Database to 8.4.3 in this release.

> **Note**
>
> In `db-monitor-svc` script, the PVC and JVM-related metrics are disabled by default. This is due to PVC and JVM metrics fetch-time exceeding the Prometheus metrics fetch-timeout. This impacts the metrics fetch cycle.
>
> The following PVC metrics are disabled:
>
> - * *db_tier_pvc_read_write_speed*
>   * *db_tier_pvc_is_accesible*
>   * *db_tier_pvc_failure_count*
>
> The following JVM metrics are disabled:
>
> - * *jvm_max_memory*
>   * *jvm_free_memory*
>   * *jvm_total_memory*

The following table lists the license names for feature mapping. For additional licensing information, see *Oracle Communications Cloud Native Core Licensing Information User Manual*.

Table 2-3 License names for feature mapping

License Name	CCNC Number	Feature Name
Oracle Communications Cloud Native Core, Network Slice Selection Function- 25K Active Subscribers Perpetual	CCNC-8876	Enhanced Georeplication Recovery using Parallel Backup Transfer and Restore
Oracle Communications Cloud Native Core, Network Slice Selection Function- 25K Active Subscribers Perpetual	CCNC-5332	Support for TLS
Oracle Communications Cloud Native Core, Policy and Charging Rules Function - 25K Subscribers Perpetual	CCNC-9356	Compatibility with two Webscale versions per release

2.5 Cloud Native Configuration Console (CNC Console)

Release 25.1.100

Oracle Communications Cloud Native Configuration Console (CNC Console) 25.1.100 includes the following enhancements:

- **Multiple Admin Support for CNCC IAM Deployments**: As CNC Console evolved from a simple interface for managing a single network function (NF) instance with one admin account to supporting multi-cluster deployments catering to multiple NF Instances including access management to observability applications, there was a need to have support for multiple admin users for managing the users across multiple customer operations teams. As part of this feature, CNC Console IAM is enhanced to support creation and management of multiple admin users in IAM using both internal and external IDPs (SAML and LDAP). For all the admin accounts managed in CNC Console, all the existing measurements, alarms, and logging mechanisms would be applicable to all admin users similar to the existing core users.

  There are default password policies defined for CNCC IAM users in the default realm. These policies are disabled by default and can be enabled, if needed.During the deployment, a default admin user is created. To create multiple CNCC IAM admin users, refer to the "*Post Installation steps*" section in *Oracle Communications Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide* and *Oracle Communications Cloud Native Configuration Console User Guide*.

The following table lists the license names for feature mapping. For additional licensing information, see *Oracle Communications Cloud Native Core Licensing Information User Manual*.

Table 2-4 License names for feature mapping

License Name	CCNC Number	Feature Name
Oracle Communications Cloud Native Core, Cloud Native Environment - per 25K Subscribers Perpetual	CCNC-9858	Multiple Admin support for CNCC IAM deployments

Table 2-4 (Cont.) License names for feature mapping

License Name	CCNC Number	Feature Name
Oracle Communications Cloud Native Core, Cloud Native Environment - per 25K Subscribers Perpetual	CCNC-8525	IAM Backend Upliftment

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

Release 25.1.100

Oracle Communications Cloud Native Core, Certificate Management (OCCM) 25.1.100 includes the following enhancements:

- **Support to Increase the Certificate Management Capacity**: OCCM is designed to manage certificates for multiple NFs. This feature increases the maximum number of supported certificates (both OCCM and NF certificates) to 200. For more information about certificate management, see the "*Managing Certificates*" section in *Oracle Communications Cloud Native Core, Certificate Management User Guide*. For more information, see "*OCCM Configuration Maximum Limits", see the "OCCM Deployment Models*" section in *Oracle Communications Cloud Native Core, Certificate Management Installation, Upgrade, and Fault Recovery Guide*.
- **Expired Certificate Handling**: This feature enables OCCM to raise alert and stop the retry of CMP (Certificate Management Protocol) Identity (OCCM) certificate renewal. For the expired End Entity (NF) certificates, if OCCM is configured to sign the Certificate Management Protocol Version 2 (CMPv2) Key Update Request (KUR) using the certificate and key that is being renewed, then OCCM raises an alert indicating the expiry of the certificate and stop the retry of NF certificate renewal. For more information, see "*Expired Certificate Handling*" section in *Oracle Communications Cloud Native Core, Certificate Management Troubleshooting Guide*.
- **Bulk Migration of Certificates:** With this feature, you can update the issuer configuration and endpoint by updating fields such as the server URL, recipient Distinguished Name (DN), and issuer DN. This update is performed by migrating the certificates in bulk from the current issuer to a newly created issuer with the required configuration. For more information, see "*Bulk Migration of Certificates*" section in *Oracle Communications Cloud Native Core, Certificate Management User Guide*.

The following table lists the license names for feature mapping. For additional licensing information, see *Oracle Communications Cloud Native Core Licensing Information User Manual*.

Table 2-5 License names for feature mapping

License Name	CCNC Number	Feature Name
Oracle Communications Cloud Native Core, Certificate Management - 25K Active Subscribers	CCNC-8810	Support to Increase the Certificate Management Capacity

Table 2-5 (Cont.) License names for feature mapping

License Name	CCNC Number	Feature Name
Oracle Communications Cloud Native Core, Certificate Management - 25K Active Subscribers	CCNC-8808	Expired Certificate Handling
Oracle Communications Cloud Native Core, Certificate Management - 25K Active Subscribers	CCNC-6075	Bulk Migration of Certificates

2.7 Network Repository Function (NRF)

Release 25.1.100

Oracle Communications Cloud Native Core, Network Repository Function (NRF) 25.1.100 includes the following enhancements:

- **Egress Gateway Pod Throttling**: With the implementation of this feature, each Egress Gateway pods monitor its incoming traffic and if the traffic exceeds the defined capacity, the excess traffic is not processed and gets rejected. This feature is applied at each pod and applicable to all the incoming requests irrespective of the message type. For more information, see the "*Egress Gateway Pod Throttling*" section in *Oracle Communications Cloud Native Core, Network Repository Function User Guide*.
- **Configuring the Stack Trace Depth**: With this feature, NRF allows the users to configure the depth of the stack trace to be logged when a Java exception occurs. For more information, see the "*Configuring the Stack Trace Depth*" section in *Oracle Communications Cloud Native Core, Network Repository Function Troubleshooting Guide*.
- **Discovery Parameter Value Based Skip SLF Lookup**: With this feature, NRF provides an option to configure a set of allowed values for the discovery query parameter. If the parameter is present in the discovery request and its value matches the configured values, the SLF lookup will be skipped. For more information about this feature, see "*Discovery Parameter Value Based Skip SLF Lookup*" section in *Oracle Communications Cloud Native Core, Network Repository Function User Guide.*
- **Traffic Segregation**: NRF supports end-to-end traffic segregation based on traffic types. This ensures that critical networks are not cross-connected or share the same routes, thereby preventing network congestion. For more information, see the "*Traffic Segregation*" section in *Oracle Communications Cloud Native Core, Network Repository Function User Guide*.
- **Support for Dual Stack**: This feature enables NRF to operate seamlessly in a Kubernetes environment configured for both IPv4 and IPv6 protocols. It facilitates the coexistence and interoperability of IPv4 and IPv6 within Kubernetes clusters, allowing simultaneous communication using either of the protocols based on the deployment configuration. For more information, see "*Dual Stack*" section in *Oracle Communications Cloud Native Core, Network Repository Function User Guide*.

The following table lists the license names for feature mapping. For additional licensing information, see *Oracle Communications Cloud Native Core Licensing Information User Manual*.

License Name	CCNC Number	Feature Name
Oracle Communications Cloud Native Core, Network Repository Function - 25K Active Subscribers Perpetual	CCNC-7898	Discovery Parameter Value Based Skip SLF Lookup
Oracle Communications Cloud Native Core, Network Repository Function - 25K Active Subscribers Perpetual	CCNC-4450	Traffic Segregation
Oracle Communications Cloud Native Core, Advance Networking - 25K Active Subscribers	CCNC-1223	Support for Dual Stack

2.8 Network Slice Selection Function (NSSF)

Release 25.1.100

Oracle Communications Cloud Native Core, Network Slice Selection Function (NSSF) 25.1.100 includes the following enhancements:

- **DNS SRV-Based Selection of NRF in NSSF:** The DNS SRV-based selection feature enhances the Network Slice Selection Function (NSSF) by introducing dynamic Network Repository Function (NRF) selection through DNS SRV records. This update improves network resilience by allowing NSSF to dynamically switch to alternate NRFs in case of primary NRF failures, ensuring continuous service availability. For more information, see the "*DNS SRV-Based Selection of NRF in NSSF*" section in *Oracle Communications Cloud Native Core, Network Slice Selection Function User Guide*.
- **Deleting All Slices in a TAI Using PATCH Remove Operation:** This feature enhances NSSF by enabling more flexible management of network slices in 5G networks. It allows the AMF to delete all slices for specific Tracking Areas (TAIs), TAILists, or TAIRanges using the PATCH operation. For more information, see the "*Deleting All Slices in a TAI Using PATCH Remove Operation*" section in *Oracle Communications Cloud Native Core, Network Slice Selection Function User Guide.*
- **Improved Error Response when All Slices are Removed:** NSSF now provides clearer responses, such as returning 204 No Content when all slices in an area are removed, while still allowing slices to be re-added through PATCH or PUT operations. This enhancement improves granularity, efficiency, and control for slice management while aligning with 3GPP standards. For more information, see the "*Deleting All Slices in a TAI Using PATCH Remove Operation*" section in *Oracle Communications Cloud Native Core, Network Slice Selection Function User Guide.*

The following table lists the license names for feature mapping. For additional licensing information, see *Oracle Communications Cloud Native Core Licensing Information User Manual*.

Table 2-6 License names for feature mapping

License Name	CCNC Number	Feature Name
Oracle Communications Cloud Native Core, Network Slice Selection Function - 25K Active Subscribers Perpetual	CCNC-4529	DNS SRV-Based Selection of NRF in NSSF

Table 2-6 (Cont.) License names for feature mapping

License Name	CCNC Number	Feature Name
Oracle Communications Cloud Native Core, Network Slice Selection Function - 25K Active Subscribers Perpetual	CCNC-9140	Deleting All Slices in a TAI Using PATCH Remove Operation
Oracle Communications Cloud Native Core, Network Slice Selection Function - 25K Active Subscribers Perpetual	CCNC-8381	Improved Error Response when All Slices are Removed
Oracle Communications Cloud Native Core, Network Slice Selection Function - 25K Active Subscribers Perpetual	CCNC-9228 CCNC-5077	Compatibility with two Webscale versions per release

2.9 Service Communication Proxy (SCP)

Release 25.1.100

Oracle Communications Cloud Native Core, Service Communication Proxy (SCP) 25.1.100 includes the following enhancements:

- **NF Discovery Response Cache Update Based on the Received Notifications**: With this enhancement, SCP can automatically refresh its Model D discovery response cache in real-time based on notifications from the NRF whenever NF profile information is updated or changed. For more information, see the "*NF Discovery Response Cache Update Based on the Received Notifications*" section in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.
- **Verbose Logging for SCP**: This enhancement introduces verbose logging specifically for the SCP-Loadmanager microservice within the data plane. For more information, see the "*Verbose Logging for SCP*" section in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.
- **Mediation Support for User Defined Variables in Rules and Trigger Points**: This enhancement allows SCP to store information at a mediation trigger point and pass it to another mediation trigger point within the same transaction. This feature is especially beneficial for complex message manipulations, such as modifying a response based on the content of the initial request. For more information, see the "*Mediation Support for User Defined Variables in Rules and Trigger Points*" section in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.
- **Alternate Routing Configuration Based on Received Status Code 504, Expired Response Timeout and Connection Error**: This feature allows you to manage alternate routing based on the response timeouts, that is, 504 errors from the upstream, and handles local errors such as timeout detected by SCP or connect errors effectively. For more information, see the "*Alternate Routing Configuration Based on Received Status Code 504, Expired Response Timeout and Connection Error*" section in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.
- **Support for 3GPP Defined NFs, Custom NFs, and Custom NF Services**: SCP enhances its capability to support the addition of new 3GPP defined NFs, custom NFs, and custom NF services at runtime using REST APIs. Also, SCP allows you to configure timers for a service based on the operation type. For more information, see the "*Support for*

3GPP Defined NFs, Custom NFs, and Custom NF Services" section in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.

- **Support for 3GPP Timestamp Related Headers**: This enhancement allows SCP to calculate the request timeout and total transaction lifetime by using the 3GPP-defined SBI Timestamp headers included in the SBI request messages. For more information, see the "*Support for 3GPP Timestamp Related Headers*" section in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.
- **Traffic Segregation**: SCP supports end-to-end traffic segregation based on traffic types. This ensures that critical networks are not cross-connected or share the same routes, thereby preventing network congestion. For more information, see the "*Traffic Segregation*" section in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.

The following table lists the license names for feature mapping. For additional licensing information, see *Oracle Communications Cloud Native Core Licensing Information User Manual*.

Table 2-7 License names for feature mapping

License Name	CCNC Number	Feature Name
Oracle Communications Cloud Native Core, Service Communication Proxy - 25K Active Subscribers Perpetual	CCNC-8267	NF Discovery Response Cache Update Based on the Received Notifications
Oracle Communications Cloud Native Core, Service Communication Proxy - 25K Active Subscribers Perpetual	CCNC-8452	Verbose Logging for SCP
Oracle Communications Cloud Native Core, Service Communication Proxy - 25K Active Subscribers Perpetual	CCNC-8150	Mediation Support for User Defined Variables in Rules and Trigger Points
Oracle Communications Cloud Native Core, Service Communication Proxy - 25K Active Subscribers Perpetual	CCNC-8265	Alternate Routing Configuration Based on Received Status Code 504, Expired Response Timeout and Connection Error
Oracle Communications Cloud Native Core, Service Communication Proxy - 25K Active Subscribers Perpetual	CCNC-7792 CCNC-7638 CCNC-4884	Support for 3GPP Defined NFs, Custom NFs, and Custom NF Services
Oracle Communications Cloud Native Core, Service Communication Proxy - 25K Active Subscribers Perpetual	CCNC-7767	Compatibility with two Webscale versions per release
Oracle Communications Cloud Native Core, Advanced Routing – 25K Active Subscribers Perpetual	CCNC-8166	Support for 3GPP Timestamp Related Headers
Oracle Communications Cloud Native Core, Advanced Cloud Native Environment – 25K Active Subscribers Perpetual	CCNC-4442	Traffic Segregation

2.10 Security Edge Protection Proxy (SEPP)

Release 25.1.102

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

Release 25.1.101

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

Release 25.1.100

Oracle Communications Cloud Native Core, Security Edge Protection Proxy (SEPP) 25.1.100 includes the following enhancements:

- **Cat-3 Time Check for Roaming Subscribers Feature**: In roaming scenarios, customers enter different time zones or regions, which must be verified. To ensure the same, SEPP uses PLMN-IDs (Public Land Mobile Network identifiers) to check if the subscriber has entered a new time zone.
  The SEPP compares the last recorded PLMN-ID from the subscriber's previous registration with the new PLMN-ID. By doing this, the SEPP can confirm if the subscriber has moved to a new time zone or area. This process ensures accurate monitoring and verification of subscriber movements while roaming. The process starts with the P-SEPP checking if the feature is enabled for the specified consumer Remote SEPP Set. This feature is specifically for AUSF UE Authentication messages and only works when the Subscription Permanent Identifier/Subscription Concealed Identifier (SUPI/SUCI) is included in the incoming message. When the SEPP receives the SBI request, it extracts key information, such as the SUPI/SUCI (UE ID), the Serving PLMN, and the Sender Timestamp. If the SUCI is present, the SEPP queries the UDM to get the corresponding SUPI. Once the SUPI is retrieved, the SEPP queries the UDR to check the subscriber’s authentication status. If the SUPI is already in the incoming message, the SEPP directly queries the UDM for the authentication status.

  For more information about the feature, see "*Cat-3 Time Check for Roaming Subscribers Feature*" section in *Oracle Communications Cloud Native Core, Security Edge Protection Proxy User Guide, Oracle Communications Cloud Native Core, Security Edge Protection Proxy REST API Guide,* and *Oracle Communications Cloud Native Core, Security Edge Protection Proxy Troubleshooting Guide*.
- **Support for Dual Stack**: This feature enables SEPP to operate seamlessly in a Kubernetes environment configured for both IPv4 and IPv6 protocols. It facilitates the coexistence and interoperability of IPv4 and IPv6 within Kubernetes clusters, allowing simultaneous communication using either of the protocols based on the deployment configuration. For more information about the feature, see the "*IPv6 Dual Stack Support*" section in *Oracle Communications Cloud Native Core, Security Edge Protection Proxy User Guide* and *Oracle Communications Cloud Native Core, Security Edge Protection Proxy REST API Guide*.
- **SEPP Message Feed Enhancement**: SEPP supports copying of the incoming and outgoing messages passing through Ingress and Egress Gateways to a Data Director. The Data Director receives the messages from Gateways with a correlation-id and feeds the data securely to an external monitoring system. From Gateway Services 25.1.100, Gateway Services are enhanced to capture all messages within a transaction onto the same Kafka partition based on the keybasedKafkaProducer Helm configuration. If `keybasedKafkaProducer` is set to true, correlation-id metadata is used as the message key for the key-based Kafka producer. This ensures that the same transaction messages are

routed to the same partition. If `keybasedKafkaProducer` is set to false, all the messages are distributed across all the available partitions in a round-robin order.
For more information about the feature, see the "*SEPP Message Feed Feature*" section in *Oracle Communications Cloud Native Core, Security Edge Protection Proxy User Guide*, "*Customizable Parameters*" in *Oracle Communications Cloud Native Core, Security Edge Protection Proxy Installation, Upgrade, and Fault Recovery Guide*.

- **ASM Upgrade:** Oracle SEPP leverages the Istio or Envoy service mesh (Aspen Service Mesh) for all internal and external communication. The ASM resource configurations are enhanced for required traffic management as per expected traffic flow. For more information about the feature, see the "*Configuring SEPP to Support Aspen Service Mesh*" section and "*Customizable Parameters*" in *Oracle Communications Cloud Native Core, Security Edge Protection Proxy Installation, Upgrade, and Fault Recovery Guide*.

The following table lists the license names for feature mapping. For additional licensing information, see *Oracle Communications Cloud Native Core Licensing Information User Manual*.

Table 2-8   License names for feature mapping

License Name	CCNC Number	Feature Name
Oracle Communications Cloud Native Core, 5G Signaling Firewall - 25K Active Subscribers Perpetual	CCNC-2830	Cat-3 Time Check for Roaming Subscribers Feature
Oracle Communications Cloud Native Core, Advance Networking - 25K Active Subscribers	CCNC-5460	Support for Dual Stack
Oracle Communications Network Analytics Data Director, Service Communication Proxy Advanced Packet Processing - Network-Wide Message per Second	CNCC-8557	SEPP Message Feed Enhancement
Oracle Communications Cloud Native Core, Security Edge Protection Proxy - 25K Active Subscribers Perpetual	CNCC-3467	ASM Upgrade
Oracle Communications Cloud Native Core, Security Edge Protection Proxy - 25K Active Subscribers Perpetual	CCNC-2715 CCNC-2714 CCNC-2711 CCNC-2710	Mano Compliance

ATS Features

SEPP ATS includes the following features or enhancements:

ATS Tagging Support Feature: This feature assists in running the feature files after filtering features and scenarios based on tags. By using this feature, the user can save time taken by manually navigating through several feature files. For more information, see the "*ATS Tagging Support Feature*" section in the *Oracle Communications Cloud Native Core, Automated Testing Suite User Guide.*

2.11 Unified Data Repository (UDR)

Release 25.1.100

Oracle Communications Cloud Native Core, Unified Data Repository (UDR) 25.1.100 includes the following enhancements:

- **Support for Post Operation for an Existing Subscription**: This feature enables UDR to support POST request that overwrites the existing subscription. For more information, see the "*Support for Post Operation for an Existing Subscription*" section in *Oracle Communications Cloud Native Core, Unified Data Repository User Guide*.
- **Support for Georeplication Recovery APIs in CNC Console**: With this enhancement, UDR can mark the disrupted cnDBTier cluster as failed, initiate georeplication recovery, and continuously monitor their status, ensuring seamless disaster recovery operations using CNC Console. For more information, see the "*Support for Georeplication Recovery APIs in CNC Console*" section in *Oracle Communications Cloud Native Core, Unified Data Repository User Guide*.
- **Traffic Segregation**: UDR supports end-to-end traffic segregation based on traffic types. This ensures that critical networks are not cross-connected or share the same routes, thereby preventing network congestion. For more information, see the "*Traffic Segregation*" section in *Oracle Communications Cloud Native Core, Unified Data Repository User Guide*.

The following table lists the license names for feature mapping. For additional licensing information, see *Oracle Communications Cloud Native Core Licensing Information User Manual*.

Table 2-9 License names for feature mapping

License Name	CCNC Number	Feature Name
Oracle Communications Cloud Native Core, Unified Data Repository - 25K Active Subscribers	CCNC-8066	Support for Post Operation for an Existing Subscription
Oracle Communications Cloud Native Core, Subscriber Location Function - 25K Active Subscribers Perpetual	CCNC-7803	Compatibility with two Webscale versions per release
Oracle Communications Cloud Native Core, Subscriber Location Function - 25K Active Subscribers Perpetual	CCNC-5906	Added support for Dns Static Entry
Oracle Communications Cloud Native Core, Subscriber Location Function - 25K Active Subscribers Perpetual	CNCC-5797	Support for Georeplication Recovery APIs in CNC Console
Oracle Communications Cloud Native Core, Unified Data Repository - 25K Active Subscribers	CNCC-4466	Support for 25K TPS on a single UDR instance
Oracle Communications Cloud Native Core, Advanced Cloud Native Environment – 25K Active Subscribers Perpetual	CNCC-4446	Traffic Segregation

3 Media and Documentation

3.1 Media Pack

This section lists the media package for Oracle Communications Cloud Native Core 3.25.1.1xx.0. 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 3.25.1.1xx.0

Description	NF Version	ATS Version	Upgrade Supported
Oracle Communications Cloud Native Core, Binding Support Function (BSF)	25.1.100	25.1.100	BSF 25.1.100 supports fresh installation and upgrade from 24.3.x, 24.2.x, and 23.4.6. 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)	25.1.100	NA	CNC Console 25.1.100 supports fresh installation and upgrade from 24.3.x, 24.2.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 25.1.100 supports SCP 25.1.100, 24.3.x, and 24.2.x. Any newly added features in Console which have NF dependency in latest release may not be available in previous release. Any newly added features in Console which have NF dependency in latest release may not be available in previous release.

Table 3-1 (Cont.) Media Pack Contents for Oracle Communications Cloud Native Core 3.25.1.1xx.0

Description	NF Version	ATS Version	Upgrade Supported
Oracle Communications Cloud Native Core, cnDBTier (cnDBTier)	25.1.103	NA	cnDBTier 25.1.103 supports fresh installation and upgrade from 24.3.x and 24.2.x. For more information, see *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, cnDBTier (cnDBTier)	25.1.102	NA	cnDBTier 25.1.102 supports fresh installation and upgrade from 24.3.x and 24.2.x. For more information, see *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, cnDBTier (cnDBTier)	25.1.101	NA	cnDBTier 25.1.101 supports fresh installation and upgrade from 24.3.x and 24.2.x. For more information, see *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, cnDBTier (cnDBTier)	25.1.100	NA	cnDBTier 25.1.100 supports fresh installation and upgrade from 24.3.x and 24.2.x. For more information, see *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Cloud Native Environment (CNE)	25.1.101	NA	CNE 25.1.101 supports fresh installation and upgrade from 24.3.x and 25.1.100. 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)	25.1.100	NA	CNE 25.1.100 supports fresh installation and upgrade from 24.3.x. For more information, see *Oracle Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Certificate Management (OCCM)	25.1.100	NA	OCCM 25.1.100 supports fresh installation and upgrade from 24.3.x and 24.2.x. For more information, see *Oracle Communications Cloud Native Core, Certificate Management Installation, Upgrade, and Fault Recovery Guide.*

Table 3-1 (Cont.) Media Pack Contents for Oracle Communications Cloud Native Core 3.25.1.1xx.0

Description	NF Version	ATS Version	Upgrade Supported
Oracle Communications Cloud Native Core, Network Repository Function (NRF)	25.1.100	25.1.100	NRF 25.1.100 supports fresh installation and upgrade from 24.3.x and 24.2.x. For more information, see *Oracle Communications Cloud Native Core, Network Repository Function Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Network Slice Selection Function (NSSF)	25.1.100	25.1.100	NSSF 25.1.100 supports fresh installation and upgrade from 24.3.x. For more information, see *Oracle Communications Cloud Native Core, Network Slice Selection Function Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Operations Services Overlay (OSO)	25.1.103	NA	OSO 25.1.103 supports fresh installation and upgrade from 24.3.x and 25.1.1xx. For more information, see *Oracle Communications Cloud Native Core, Operations Services Overlay Installation and Upgrade Guide*.
Oracle Communications Operations Services Overlay (OSO)	25.1.102	NA	OSO 25.1.102 supports fresh installation and upgrade from 24.3.x and 25.1.1xx. For more information, see *Oracle Communications Cloud Native Core, Operations Services Overlay Installation and Upgrade Guide.*
Oracle Communications Operations Services Overlay (OSO)	25.1.101	NA	OSO 25.1.101 supports fresh installation and upgrade from 24.3.x and 25.1.100. For more information, see *Oracle Communications Cloud Native Core, Operations Services Overlay Installation and Upgrade Guide.*
Oracle Communications Operations Services Overlay (OSO)	25.1.100	NA	OSO 25.1.100 supports fresh installation and upgrade from 24.3.x. For more information, see *Oracle Communications Operations Services Overlay Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core, Service Communications Proxy (SCP)	25.1.100	25.1.100	SCP 25.1.100 supports fresh installation and upgrade from 24.3.x and 24.2.x. For more information, see *Oracle Communications Cloud Native Core, Service Communication Proxy Installation, Upgrade, and Fault Recovery Guide*.

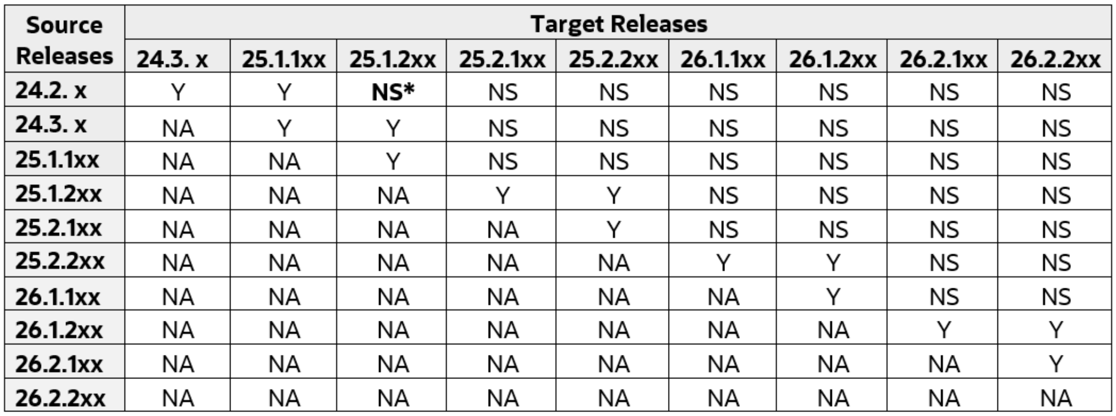
Table 3-1 (Cont.) Media Pack Contents for Oracle Communications Cloud Native Core 3.25.1.1xx.0

Description	NF Version	ATS Version	Upgrade Supported
Oracle Communications Cloud Native Core, Security Edge Protection Proxy (SEPP)	25.1.102	25.1.102	SEPP 25.1.102 supports fresh installation and upgrade from 25.1.1xx, 24.3.x, and 24.2.x. For more information, see *Oracle Communications Cloud Native Core, Security Edge Protection Proxy Installation, Upgrade, and Fault Recovery Guide.*
Oracle Communications Cloud Native Core, Security Edge Protection Proxy (SEPP)	25.1.101	25.1.102	SEPP 25.1.101 supports fresh installation and upgrade from 25.1.100, 24.3.x, and 24.2.x. For more information, see *Oracle Communications Cloud Native Core, Security Edge Protection Proxy Installation, Upgrade, and Fault Recovery Guide.*
Oracle Communications Cloud Native Core, Security Edge Protection Proxy (SEPP)	25.1.101	25.1.101	SEPP 25.1.101 supports fresh installation and upgrade from 25.1.100, 24.3.x, and 24.2.x. For more information, see *Oracle Communications Cloud Native Core, Security Edge Protection Proxy Installation, Upgrade, and Fault Recovery Guide.*
Oracle Communications Cloud Native Core, Security Edge Protection Proxy (SEPP)	25.1.100	25.1.100	SEPP 25.1.100 supports fresh installation and upgrade from 24.3.x and 24.2.x. For more information, see *Oracle Communications Cloud Native Core, Security Edge Protection Proxy Installation, Upgrade, and Fault Recovery Guide.*
Oracle Communications Cloud Native Core, Unified Data Repository (UDR)	25.1.100	25.1.100	UDR 25.1.100 supports fresh installation and upgrade from 24.3.x and 24.2.x. For more information, see *Oracle Communications Cloud Native Core, Unified Data Repository Installation, Upgrade, and Fault Recovery Guide*.

Cloud Native Core Upgrade

To ensure a smooth and supported upgrade process, follow the upgrade sequence outlined in the table below. Product does not recommend skipping intermediate versions unless explicitly showed:

Figure 3-1 Cloud Native Core Upgrade

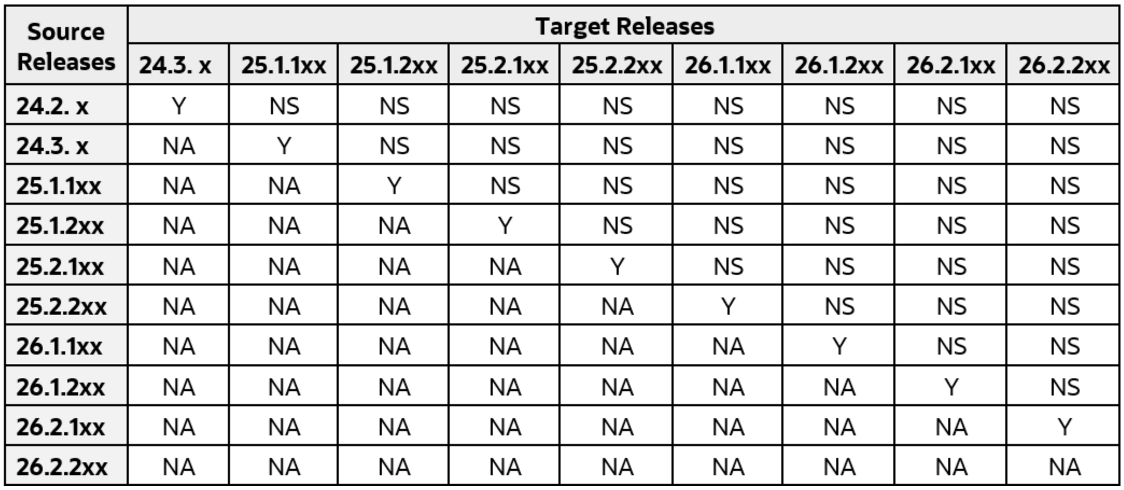


Source Releases	Target Releases								
	24.3. x	25.1.1xx	25.1.2xx	25.2.1xx	25.2.2xx	26.1.1xx	26.1.2xx	26.2.1xx	26.2.2xx
24.2. x	Y	Y	NS*	NS	NS	NS	NS	NS	NS
24.3. x	NA	Y	Y	NS	NS	NS	NS	NS	NS
25.1.1xx	NA	NA	Y	NS	NS	NS	NS	NS	NS
25.1.2xx	NA	NA	NA	Y	Y	NS	NS	NS	NS
25.2.1xx	NA	NA	NA	NA	Y	NS	NS	NS	NS
25.2.2xx	NA	NA	NA	NA	NA	Y	Y	NS	NS
26.1.1xx	NA	NA	NA	NA	NA	NA	Y	NS	NS
26.1.2xx	NA	NA	NA	NA	NA	NA	NA	Y	Y
26.2.1xx	NA	NA	NA	NA	NA	NA	NA	NA	Y
26.2.2xx	NA	NA	NA	NA	NA	NA	NA	NA	NA

CNE Upgrade

To ensure a smooth and supported upgrade process, follow the upgrade sequence outlined in the following table:

Figure 3-2 CNE Upgrade



Source Releases	Target Releases								
	24.3. x	25.1.1xx	25.1.2xx	25.2.1xx	25.2.2xx	26.1.1xx	26.1.2xx	26.2.1xx	26.2.2xx
24.2. x	Y	NS	NS	NS	NS	NS	NS	NS	NS
24.3. x	NA	Y	NS	NS	NS	NS	NS	NS	NS
25.1.1xx	NA	NA	Y	NS	NS	NS	NS	NS	NS
25.1.2xx	NA	NA	NA	Y	NS	NS	NS	NS	NS
25.2.1xx	NA	NA	NA	NA	Y	NS	NS	NS	NS
25.2.2xx	NA	NA	NA	NA	NA	Y	NS	NS	NS
26.1.1xx	NA	NA	NA	NA	NA	NA	Y	NS	NS
26.1.2xx	NA	NA	NA	NA	NA	NA	NA	Y	NS
26.2.1xx	NA	NA	NA	NA	NA	NA	NA	NA	Y
26.2.2xx	NA	NA	NA	NA	NA	NA	NA	NA	NA

3.2 Compatibility Matrix

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

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

Table 3-2 Compatibility Matrix

CNC NF	NF Version	CNE	cnDBTier	OSO	ASM S/W	Kubernetes	CNC Console	OCNADD	OCCM	OCI Adaptor
BSF	25.1.100	• 25.1.1xx • 24.3.x • 24.2.x	• 25.1.1xx • 24.3.x • 24.2.x	• 25.1.1xx • 24.3.x • 24.2.x	1.14.6	• 1.31.x • 1.30.x • 1.29.x	25.1.1xx	25.1.1xx	25.1.1xx	NA
CNC Console	25.1.100	• 25.1.1xx • 24.3.x • 24.2.x	• 25.1.1xx • 24.3.x • 24.2.x	• 25.1.1xx • 24.3.x • 24.2.x	• 1.14.6 • 1.11.8 • 1.9.8	• 1.31.x • 1.30.x • 1.29.x	NA	25.1.1xx	25.1.1xx	24.3.x
cnDBTier	25.1.103	• 25.1.1xx • 24.3.x • 24.2.x	NA	NA	NA	• 1.31.x • 1.30.x • 1.29.x	NA	NA	NA	NA
cnDBTier	25.1.102	• 25.1.1xx • 24.3.x • 24.2.x	NA	NA	NA	• 1.31.x • 1.30.x • 1.29.x	NA	NA	NA	NA
cnDBTier	25.1.101	• 25.1.1xx • 24.3.x • 24.2.x	NA	NA	NA	• 1.31.x • 1.30.x • 1.29.x	NA	NA	NA	NA
cnDBTier	25.1.100	• 25.1.1xx • 24.3.x • 24.2.x	NA	NA	NA	• 1.31.x • 1.30.x • 1.29.x	NA	NA	NA	NA
CNE	25.1.100	NA	NA	NA	NA	1.31.x	NA	NA	NA	NA
CNE	25.1.100	NA	NA	NA	NA	1.31.x	NA	NA	NA	NA

Table 3-2 (Cont.) Compatibility Matrix

CNC NF	NF Version	CNE	cnDBTier	OSO	ASM S/W	Kubernetes	CNC Console	OCNADD	OCCM	OCI Adaptor
NRF	25.1.100	• 25.1.1xx • 24.3.x • 24.2.x	• 25.1.1xx • 24.3.x • 24.2.x	• 25.1.1xx • 24.3.x • 24.2.x	1.14.6	• 1.31.x • 1.30.x • 1.29.x	25.1.1xx	25.1.1xx	25.1.1xx	24.3.x
NSSF	25.1.100	• 25.1.1xx • 24.3.x • 24.2.x	• 25.1.1xx • 24.3.x • 24.2.x	• 25.1.1xx • 24.3.x • 24.2.x	• 1.14.6 • 1.11.8	• 1.31.x • 1.30.x • 1.29.x	25.1.1xx	NA	NA	NA
OCCM	25.1.100	• 25.1.1xx • 24.3.x • 24.2.x	NA	NA	NA	• 1.30.x • 1.29.x • 1.28.x	23.4.x	NA	NA	NA
OSO	25.1.103	NA	NA	NA	NA	• 1.31.x • 1.30.x • 1.29.x	NA	NA	NA	NA
OSO	25.1.102	NA	NA	NA	NA	• 1.31.x • 1.30.x • 1.29.x	NA	NA	NA	NA
OSO	25.1.101	NA	NA	NA	NA	• 1.31.x • 1.30.x • 1.29.x	NA	NA	NA	NA
OSO	25.1.100	NA	NA	NA	NA	• 1.31.x • 1.30.x • 1.29.x	NA	NA	NA	NA

Table 3-2 (Cont.) Compatibility Matrix

CNC NF	NF Version	CNE	cnDBTier	OSO	ASM S/W	Kubernetes	CNC Console	OCNADD	OCCM	OCI Adaptor
SCP	25.1.100	• 25.1.1xx • 24.3.x • 24.2.x	• 25.1.1xx • 24.3.x • 24.2.x	• 25.1.1xx • 24.3.x • 24.2.x	• 1.14.6 • 1.11.8	• 1.31.x • 1.30.x • 1.29.x	25.1.1xx	25.1.1xx	25.1.1xx	24.3.x
SEPP	25.1.102	• 25.1.1xx • 24.3.x • 24.2.x	• 25.1.1xx • 24.3.x • 24.2.x	25.1.1xx	1.14.6	• 1.31.x • 1.30.x • 1.29.x	25.1.1xx	NA	25.1.1xx	24.3.x
SEPP	25.1.101	• 25.1.1xx • 24.3.x • 24.2.x	• 25.1.1xx • 24.3.x • 24.2.x	25.1.1xx	1.14.6	• 1.31.x • 1.30.x • 1.29.x	25.1.1xx	NA	25.1.1xx	24.3.x
SEPP	25.1.100	• 25.1.1xx • 24.3.x • 24.2.x	• 25.1.1xx • 24.3.x • 24.2.x	25.1.1xx	1.14.6	• 1.31.x • 1.30.x • 1.29.x	25.1.1xx	NA	25.1.1xx	24.3.x
UDR	25.1.100	• 25.1.1xx • 24.3.x • 24.2.x	• 25.1.1xx • 24.3.x • 24.2.x	• 25.1.1xx • 24.3.x • 24.2.x	• 1.1.4.6 • 1.11.8	• 1.31.x • 1.30.x • 1.29.x	25.1.1xx	NA	25.1.1xx	NA

3.3 3GPP Compatibility Matrix

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

Table 3-3 3GPP Compatibility Matrix

CNC NF	NF Version	3GPP
BSF	25.1.100	• 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	25.1.100	NA
cnDBTier	25.1.1xx	NA
cnDBTier	25.1.100	NA
CNE	25.1.1xx	NA
NSSF	25.1.100	• 3GPP TS 29.531 v15.5.0 • 3GPP TS 29.531 v16.5.0 • 3GPP TS 29.531 v16.8.0 • 3GPP TS 29.501 v16.10.0 • 3GPP TS 29.502 v16.10.0
OCCM	25.1.100	• 3GPP TS 33.310-h30 • 3GPP TR 33.876 v.0.3.0
OSO	25.1.1xx	NA
SCP	25.1.100	3GPP TS 29.500 v17.12.0
SEPP	25.1.1xx	• 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	25.1.100	• 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 3.25.1xx.0.

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	25.1.100	25.1.102	25.1.102	25.1.100	25.1.102	25.1.102	25.1.101	25.1.102	25.1.102	25.1.101	NA	25.1.102	25.1.102
CNC Console	25.1.100	NA	NA	NA	NA	NA	25.1.101	NA	25.1.101	25.1.101	NA	NA	NA
OCCM	25.1.100	NA	NA	NA	NA	NA	25.1.101	NA	NA	25.1.101	NA	NA	NA
NRF	25.1.100	25.1.103	25.1.101	25.1.100	25.1.100	NA	25.1.101	25.1.103	25.1.103	25.1.101	NA	NA	25.1.101
NSSF	25.1.100	25.1.102	25.1.101	25.1.100	25.1.102	25.1.101	25.1.101	25.1.102	25.1.102	25.1.101	NA	25.1.102	25.1.101
SCP	25.1.100	NA	NA	25.1.100	25.1.102	NA	25.1.101	NA	NA	25.1.101	25.1.103	NA	NA
SEPP	25.1.102	25.1.103	25.1.101	25.1.100	25.1.102	25.1.101	25.1.101	25.1.103	25.1.103	25.1.102	25.1.103	25.1.102	25.1.101
SEPP	25.1.101	25.1.103	25.1.101	25.1.100	25.1.102	25.1.101	25.1.101	25.1.103	25.1.103	25.1.102	25.1.103	25.1.102	25.1.101
SEPP	25.1.100	25.1.103	25.1.101	25.1.100	25.1.102	25.1.101	25.1.101	25.1.103	25.1.103	25.1.102	25.1.103	25.1.102	25.1.101
UDR	25.1.100	25.1.102	25.1.101	25.1.100	25.1.102	25.1.101	25.1.101	25.1.102	25.1.102	25.1.102	NA	25.1.102	25.1.101

3.5 Generic Open Source Software Compatibility on Any Platform

The following table offers a comprehensive list of software necessary for the proper functioning of an NF during deployment. However, this table is indicative, and the software used may vary based on the customer's specific requirements and solution.

> **Note**
>
> The Software Requirement column in the following table indicates one of the following:
>
> - Mandatory: Absolutely essential; the software cannot function without it.
> - Recommended: Suggested for optimal performance or best practices but not strictly necessary.
> - Conditional: Required only under specific conditions or configurations.
> - Optional: Not essential; can be included based on specific use cases or preferences.

Table 3-5 Generic Open Source Software Compatibility on Any Platform

Software	Tested Software Version			Software Requirement	Category	Sub-Category	Category Requirement	Usage Description
	NF 25.1.1xx	NF 24.3.x	NF 24.2.x					
Kubernetes	1.31	1.30	1.29.1	Mandatory	Orchestration	Container Orchestration	Mandatory	Kubernetes orchestrates scalable, automated NF deployments for high availability and efficient resource utilization. **Impact**: Preinstallation is required. Without orchestration capabilities, deploying and managing network functions (NFs) can become complex, leading to inefficient resource utilization and potential downtime.
Helm	3.16.2	3.15.2	3.13.2	Mandatory	Management	Kubernetes Package Management	Mandatory	Helm, a package manager, simplifies deploying and managing NFs on Kubernetes with reusable, versioned charts for easy automation and scaling. **Impact**: Preinstallation is required. Not using this capability may result in error-prone and time-consuming management of NF versions and configurations, impacting deployment consistency.

Table 3-5 (Cont.) Generic Open Source Software Compatibility on Any Platform

Software	Tested Software Version			Software Requirement	Category	Sub-Category	Category Requirement	Usage Description
	NF 25.1.1xx	NF 24.3.x	NF 24.2.x					
Podman		4.9.4		Recommended	Runtime	Containerized NF Image Management	Mandatory	Podman manages and runs containerized NFs without requiring a daemon, offering flexibility and compatibility with Kubernetes. **Impact**: Preinstallation is required. Podman is a part of Oracle Linux. Without efficient container management, the development and deployment of NFs could become cumbersome, impacting agility.
containerd	1.7.22	1.7.16	1.7.13	Recommended	Runtime	Container Runtime	Mandatory	Containerd manages container lifecycles for running NFs efficiently in Kubernetes. **Impact**: A lack of a reliable container runtime could lead to performance issues and instability in NF operations.
Velero	1.13.2	1.12.0	1.12.0	Recommended	Backup	Backup and Disaster Recovery for Kubernetes	Optional	Velero backs up and restores Kubernetes clusters for 5G NFs, ensuring data protection and disaster recovery. **Impact**: Without backup and recovery capabilities, customers would risk data loss and extended downtime, requiring a full cluster reinstall in case of failure or upgrade.

Table 3-5 (Cont.) Generic Open Source Software Compatibility on Any Platform

Software	Tested Software Version			Software Requirement	Category	Sub-Category	Category Requirement	Usage Description
	NF 25.1.1xx	NF 24.3.x	NF 24.2.x					
Kyverno	1.12.5	1.12.5	1.9	Recommended	Security	Kubernetes Policy Management	Mandatory	Kyverno is a Kubernetes policy engine that allows to manage and enforce policies for resource configurations within a Kubernetes cluster. **Impact**: Failing to implement policy enforcement could lead to misconfigurations, resulting in security risks and instability in NF operations, affecting reliability.
MetalLB	0.14.4	0.14.4	0.14.4	Recommended	Networking	Load Balancer for Kubernetes	Mandatory	MetalLB provides load balancing and external IP management for 5G NFs in Kubernetes environments. **Impact**: MetalLB is used as LB solution in CNE. LB is mandatory for the solution to work. Without load balancing, traffic distribution among NFs may be inefficient, leading to potential bottlenecks and service degradation.

Table 3-5 (Cont.) Generic Open Source Software Compatibility on Any Platform

Software	Tested Software Version			Software Requirement	Category	Sub-Category	Category Requirement	Usage Description
	NF 25.1.1xx	NF 24.3.x	NF 24.2.x					
HAProxy		3.0.2		Recommended	Networking	Load Balancer / Reverse Proxy	Mandatory	HAProxy provides load balancing and high availability for 5G NFs, ensuring efficient traffic distribution and reliability. **Impact**: HAProxy is used as LB solution in CNE. LB is mandatory for the solution to work. Absense of effective traffic management could result in poor service distribution, impacting NF performance and leading to service interruptions.
CoreDNS	1.11.1	1.11.1	1.10.1	Recommended	Networking	Service Discovery for Kubernetes	Mandatory	CoreDNS is the DNS server in Kubernetes, which provides DNS resolution services within the cluster. **Impact**: DNS is an essential part of deployment. Without proper service discovery, NFs would struggle to communicate with each other, leading to connectivity issues and operational failures.

Table 3-5 (Cont.) Generic Open Source Software Compatibility on Any Platform

Software	Tested Software Version			Software Requirement	Category	Sub-Category	Category Requirement	Usage Description
	NF 25.1.1xx	NF 24.3.x	NF 24.2.x					
Multus	3.8	3.8.0	3.8.0	Recommended	Networking	Networking for Kubernetes traffic segregation	Conditional	Multus enables multiple network interfaces in Kubernetes pods, allowing custom configurations and isolated paths for advanced use cases such as NF deployments, ultimately supporting traffic segregation. **Impact**: Without this capability, connecting NFs to multiple networks could be limited, impacting network performance and isolation.
Fluentd	1.17.1	1.16.2	1.16.2	Recommended	Logging	Logging Agent	Mandatory	Fluentd is an open-source data collector that streamlines data collection and consumption, allowing for improved data utilization and comprehension. **Impact**: Not utilizing centralized logging can hinder the ability to track NF activity and troubleshoot issues effectively, complicating maintenance and support.
OpenSearch	2.11.0	2.11.0	2.11.0	Recommended	Logging	Search/ Analytics / Logging	Mandatory	OpenSearch provides scalable search and analytics for 5G NFs, enabling efficient data exploration and visualization. Lack of a robust analytics solution could lead to challenges in identifying performance issues and optimizing NF operations, affecting overall service quality.

Table 3-5 (Cont.) Generic Open Source Software Compatibility on Any Platform

Software	Tested Software Version			Software Requirement	Category	Sub-Category	Category Requirement	Usage Description
	NF 25.1.1xx	NF 24.3.x	NF 24.2.x					
OpenSearch Dashboard	2.11.0	2.11.0	2.11.0	Recommended	Logging	Dashboard/ Visualization for OpenSearch	Mandatory	OpenSearch Dashboard visualizes and analyzes data for 5G NFs, offering interactive insights and custom reporting. **Impact**: Without visualization capabilities, understanding NF performance metrics and trends would be difficult, limiting informed decision-making.
AlertManager	0.27.0	0.27.0	0.27.0	Recommended	Alerting	Alerting (Integration with Prometheus)	Mandatory	Alertmanager is a component that works in conjunction with Prometheus to manage and dispatch alerts. It handles the routing and notification of alerts to various receivers. **Impact**: Not implementing alerting mechanisms can lead to delayed responses to critical issues, potentially resulting in service outages or degraded performance.
prometheus-kube-state-metric	2.13.0	2.13.0	2.10.1	Recommended	Monitoring	Kubernetes Metrics (for Prometheus)	Mandatory	Kube-state-metrics is a service that generates metrics about the state of various resources in a Kubernetes cluster. It's commonly used for monitoring and alerting purposes. **Impact**: Without these metrics, monitoring the health and performance of NFs could be challenging, making it harder to proactively address issues.

Table 3-5 (Cont.) Generic Open Source Software Compatibility on Any Platform

Software	Tested Software Version			Software Requirement	Category	Sub-Category	Category Requirement	Usage Description
	NF 25.1.1xx	NF 24.3.x	NF 24.2.x					
Prometheus Operator	0.76.0	0.76.0	0.72.0	Recommended	Monitoring	Prometheus Instance Management in Kubernetes	Conditional	The Prometheus Operator is used for managing Prometheus monitoring systems in Kubernetes. Prometheus Operator simplifies the configuration and management of Prometheus instances. **Impact**: Not using this operator could complicate the setup and management of monitoring solutions, increasing the risk of missed performance insights.
prometheus-node-exporter	1.8.2	1.8.2	1.7.0	Recommended	Monitoring	Node-Level Metrics for Prometheus	Mandatory	Node Exporter is a Prometheus exporter for collecting hardware and OS-level metrics from Linux hosts. **Impact**: Without node-level metrics, visibility into infrastructure performance would be limited, complicating the identification of resource bottlenecks.
Prometheus	2.52	2.52	2.51.1	Mandatory	Monitoring	Metrics/Monitoring System	Mandatory	Prometheus is a popular open-source monitoring and alerting toolkit. It collects and stores metrics from various sources and allows for alerting and querying. **Impact**: Not employing this monitoring solution could result in a lack of visibility into NF performance, making it difficult to troubleshoot issues and optimize resource usage.

Table 3-5 (Cont.) Generic Open Source Software Compatibility on Any Platform

Software	Tested Software Version			Software Requirement	Category	Sub-Category	Category Requirement	Usage Description
	NF 25.1.1xx	NF 24.3.x	NF 24.2.x					
Grafana	9.5.3	9.5.3	9.5.3	Recommended	Visualization	Monitoring/ Visualization Tool	Mandatory	Grafana is a popular open-source platform for monitoring and observability. It provides a user-friendly interface for creating and viewing dashboards based on various data sources. **Impact**: Without visualization tools, interpreting complex metrics and gaining insights into NF performance would be cumbersome, hindering effective management.
Calico	3.28.1	3.27.3	3.26.4	Recommended	Networking	Networking/ Network Security for Kubernetes	Mandatory	Calico provides networking and security for NFs in Kubernetes with scalable, policy-driven connectivity. **Impact**: CNI is mandatory for the functioning of 5G NFs. Without CNI and proper plugin, the network could face security vulnerabilities and inadequate traffic management, impacting the reliability of NF communications
metrics-server	0.7.2	0.7.1	0.6.1	Recommended	Monitoring	Resource Metrics for Kubernetes	Mandatory	Metrics server is used in Kubernetes for collecting resource usage data from pods and nodes. **Impact**: Without resource metrics, auto-scaling and resource optimization would be limited, potentially leading to resource contention or underutilization.

Table 3-5 (Cont.) Generic Open Source Software Compatibility on Any Platform

Software	Tested Software Version			Software Requirement	Category	Sub-Category	Category Requirement	Usage Description
	NF 25.1.1xx	NF 24.3.x	NF 24.2.x					
snmp-notifier	1.5.0	1.4.0	1.4.0	Recommended	Notification	SNMP Notification Service	Mandatory	snmp-notifier sends SNMP alerts for 5G NFs, providing real-time notifications for network events. **Impact**: Without SNMP notifications, proactive monitoring of NF health and performance could be compromised, delaying response to critical issues.
Jaeger	1.60.0	1.60.0	1.52.0	Recommended	Tracing	Distributed Tracing	Mandatory	Jaeger provides distributed tracing for 5G NFs, enabling performance monitoring and troubleshooting across microservices. **Impact**: Not utilizing distributed tracing may hinder the ability to diagnose performance bottlenecks, making it challenging to optimize NF interactions and user experience.
CSI	NA	NA	NA	Mandatory	Storage	Distributed, Orchestrated, and Block Storage	Mandatory	Provides scalable object, block, and file storage, with orchestration capabilities and block storage provisioning for persistent storage in Kubernetes. **Impact**: CSI is mandatory for the functioning of 5G NFs. Without CSI, managing storage could lead to data loss, inefficiencies, and challenges in scaling storage systems effectively.

Table 3-5 (Cont.) Generic Open Source Software Compatibility on Any Platform

Software	Tested Software Version			Software Requirement	Category	Sub-Category	Category Requirement	Usage Description
	NF 25.1.1xx	NF 24.3.x	NF 24.2.x					
ceph	18.2.1	18.2.1		Recommended	Storage	Distributed Storage	Mandatory	The ceph storage system offers scalable object, block, and file storage. It is used in bm CNE solution. **Impact**: Ceph is used in bm OCCNE solution. CSI is mandatory for the solution to work. Not using this distributed storage system would complicate data management, leading to potential data loss and challenges in handling large data volumes effectively.
rook	1.15.2	1.13.3	1.13.3	Recommended	Storage	Storage Orchestration	Mandatory	Rook is the Ceph orchestrator for Kubernetes that provides storage solutions. It is used in bm CNE solution. **Impact**: CSI is mandatory for the solution to work. Not utilizing Rook could increase the complexity of deploying and managing Ceph, making it difficult to scale storage solutions in a Kubernetes environment.

Table 3-5 (Cont.) Generic Open Source Software Compatibility on Any Platform

Software	Tested Software Version			Software Requirement	Category	Sub-Category	Category Requirement	Usage Description
	NF 25.1.1xx	NF 24.3.x	NF 24.2.x					
cinder-csi-plugin	1.31.1	1.30.0	1.29.0	Recommended	Storage	Block Storage Plugin	Mandatory	Cinder CSI (Container Storage Interface) plugin is for provisioning and managing block storage in Kubernetes. It is often used in OpenStack environments to provide persistent storage for containerized applications. **Impact**: Cinder CSI Plugin is used in OpenStack vCNE solution. Without this integration, provisioning block storage for NFs could be manual and inefficient, complicating storage management.

3.6 Security Certification Declaration

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

3.6.1 BSF Security Certification Declaration

Release 25.1.100

Table 3-6 BSF Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	Apr 1, 2025	No unmitigated critical or high findings

Table 3-6 (Cont.) BSF Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	Feb 18, 2025	No unmitigated critical or high findings
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	Apr 1, 2025	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	Apr 7, 2025	No findings

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

3.6.2 CNC Console Security Certification Declaration

Release 25.1.100

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	Mar 25, 2025	No unmitigated critical or high findings
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	Apr 2, 2025	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 2, 2025	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	Apr 2, 2025	No findings

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

3.6.3 OCCM Security Certification Declaration

Release 25.1.100

Table 3-8 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 2, 2025	No unmitigated critical or high findings
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	Apr 2, 2025	No unmitigated critical or high findings
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	Apr 2, 2025	No unmitigated critical or high finding

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

Compliance Test Description	Test Completion Date	Summary
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	Apr 2, 2025	No findings

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

3.6.4 NRF Security Certification Declaration

Release 25.1.100

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

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

3.6.5 NSSF Security Certification Declaration

Release 25.1.100

Table 3-10 NSSF Security Certification Declaration

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

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

3.6.6 SCP Security Certification Declaration

Release 25.1.100

Table 3-11 SCP Security Certification Declaration

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

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

3.6.7 SEPP Security Certification Declaration

Release 25.1.102

Table 3-12 SEPP Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	July 22, 2025	No unmitigated critical or high findings. Scan done through Fortify.
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	April 7, 2025	No unmitigated critical, high, medium, and low findings. Scan done through RestFuzz.
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	April 7, 2025	No unmitigated critical or high findings. Scan done through Blackduck.
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	July 22, 2025	No issues found. Scan done through McAfee.

Release 25.1.101

Table 3-13 SEPP Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	June 9, 2025	No unmitigated critical or high findings. Scan done through Fortify.
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	Dec 16, 2024	No unmitigated critical, high, medium, and low findings. Scan done through RestFuzz.

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

Compliance Test Description	Test Completion Date	Summary
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	April 7, 2025	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	June 9, 2025	No issues found. Scan done through McAfee.

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

Release 25.1.100

Table 3-14 SEPP Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	Apr 7, 2025	No unmitigated critical or high findings. Scan done through Fortify.
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	Dec 16, 2024	No unmitigated critical, high, medium, and low findings. Scan done through RestFuzz.
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	Apr 7, 2025	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	Apr 8, 2025	No issues found. Scan done through McAfee.

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

3.6.8 UDR Security Certification Declaration

Release 25.1.100

Table 3-15 UDR Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	Mar 31, 2025	No unmitigated critical or high findings
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	Mar 31, 2025	No unmitigated critical or high findings
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	Mar 31, 2025	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	Mar 31, 2025	No findings

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

3.7 Documentation Pack

All documents for Oracle Communications Cloud Native Core (CNC) 3.25.1.1xx.0 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 3.25.1.1xx.0.

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 3.25.1.1xx.0.

4.2.1 BSF Resolved Bugs

Release 25.1.100

Table 4-1 BSF 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37291979	Post BSF upgrade Over load congestion	Multiple *3004 Diameter Too Busy* error messages were causing overload congestion alarm. **Doc Impact**: There is no doc impact.	1	23.4.4
37773183	No health request going out from egress GW to scp as expected	There were no health requests going out from Egress Gateway to SCP. **Doc Impact**: There is no doc impact.	2	23.4.4
37155277	Duplicate bindng makes AAR fails with 5012 DIAMETER_UNABLE_TO_COMPLY	Authorization Authentication Request (AAR) failed with *5012 DIAMETER_UNABLE_TO_COMPLY* error message due to duplicate binding. **Doc Impact**: There is no doc impact.	3	24.2.0
37444668	BSF generating SYSTEM_OPERATIONAL_STATE_NORMAL alert	If the system was running in normal state, then `SYSTEM_OPERATIONAL_STATE_NORMAL` alert was getting triggered but it was not getting cleared. **Doc Impact**: There is no doc impact.	3	24.2.1

Table 4-1 (Cont.) BSF 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37508079	BSF REST API incorrect path for Controlled Shutdown	The REST API for controlled shutdown had incorrect path. **Doc Impact**: Updated the REST API path for controlled shutdown. For more information, see "Controlled Shutwown at Ingress and Diameter Gateway" section in *Oracle Communications Cloud Native Core, Binding Support Function REST Specification Guide*.	4	24.2.1

ⓘ **Note**

Resolved bugs from 24.2.2 have been forward ported to Release 25.1.100.

Table 4-2 BSF ATS 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37312003	Perfinfo_Overload_Manager scenario is failing	The `Perfinfo_Overload_Manager` scenario was failing.	3	24.2.1
37313029	Unexpected ServiceAccount Creation of ATS	There was an unexpected global keyword added in the ATS Helm charts as part of ATS base image integration. As a result, Helm charts were not able to find the custom service account name set in `custom_values.yaml` file.	3	24.3.0

4.2.2 CNC Console Resolved Bugs

Release 25.1.100

Table 4-3 CNC Console 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37486049	Route Path exceeding length for GW metrics	The length for `Route_path` in CNC Console metrics exceeded the limit, which caused the OSO prom-svr to fail after the CNC Console upgrade. **Doc Impact**: There is no doc impact.	2	24.2.0
37496319	Improvements in CNCC upgrade/ rollback procedure	The CNC Console upgrade and rollback procedure needed updates to improve clarity and ensure a better understanding of the process. **Doc Impact**: Updated the procedure in *M-CNCC IAM DB Rollback or Restore* section of *Oracle Communications Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide.*	2	25.1.100

Table 4-3 (Cont.) CNC Console 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37486298	CNCC 24.2.1 Installation guide documentation queries	• The cnDBTier note has to be updated to set "ndb_allow_copying_alter_table" to ON during Console deployment. • CNC Console Alert configuration in Prometheus section in *Oracle Communications Cloud Native Configuration Console User Guide* had to be updated to include a note about updating the alert rules file to change the default namespace to the Console deployed namespace. **Doc Impact**: Updated the note about the `ndb_allow_copying_alter_table` parameter in *Configuring Database* section of *Oracle Communications Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide*.	3	24.2.1

Table 4-3 (Cont.) CNC Console 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37468422	CNCC 24.3.0 Metric not displayed for one of the A-CNCC Query due to duplicate RefId	The CNC Console metric dashboard file had a duplicate Reference ID. The dashboard file has to be updated to remove the duplicate Referece ID, making each entry unique. **Doc Impact**: There is no doc impact.	3	24.3.0
37465056	CNCC 24.1.0 CncclamIngressGatewayServiceDown alert active in aCore deployment	When deploying CNC Console as an aCore only, the `CnccIamIngressGatewayServiceDown` alert was always triggered due to the absence of the IAM pod. **Doc Impact**: Updated the note about the `occncc_agent_alertrules_.yaml` file and e `occncc_manager_alertrules_.yaml` file in *CNC Console Alerts* section of Oracle Communications Cloud Native Configuration Console User Guide.	3	24.1.0
37596832	Wrong MIB file not corresponding SNMP-Notifier sent info in the alert trap towards SNMP server	The wrong MIB file, which did not correspond to the SNMP-Notifier, was sent in the alert trap towards the SNMP server. **Doc Impact**: There is no doc impact.	3	24.2.0

Table 4-3   (Cont.) CNC Console 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37649019	Avoid printing payload in security logs if its gets too large	Large response payloads were printed in security logs and stored in memory which could have caused OOM (Out of Memory) issues during high loads. **Doc Impact**: There is no doc impact.	3	25.1.100
37316800	CNCC 23.4.1 Helm Chart does not pass Helm Strict linting	The Helm chart did not pass Helm strict linting. The customer ran YAML lint on the Console Helm charts and reported multiple "duplication of key" errors. **Doc Impact**: There is no doc impact.	4	23.4.1
37306647	Upgrading CNCC documentation makes no mention of uploading target version images	The "Upgrading CNC Console" section of the *Oracle Communications Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide* had to be updated to include the step for uploading the target version images. **Doc Impact**: Updated the procedure in *Upgrading CNC Console* section of *Oracle Communications Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide*.	4	24.3.0

> **Note**
>
> Resolved bugs from 24.3.0 have been forward ported to Release 25.1.100.

4.2.3 cnDBTier Resolved Bugs

Release 25.1.103

Table 4-4 cnDBTier 25.1.103 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38220013	dbtrecover script is affecting db-monitor-svc	A deadlock occurred in the db-monitor-svc during SQL pod restart that caused connection assignment failure, as the monitoring service was unable to assign connections correctly. **Doc Impact**: There is no doc impact.	2	25.1.100
38224168	Update georeplication recovery procedure to remove duplicate steps	Updated the georeplication recovery procedure to remove the duplicated steps. **Doc Impact**: Removed the steps that mention about the creation of NFs during georeplication failure recovery. For more information see the *Restoring Georeplication (GR) Failure* section in Oracle Communications Cloud Native Core cnDBTier Installation, Upgrade, and Fault Recovery Guide.	2	25.1.102

Table 4-4 (Cont.) cnDBTier 25.1.103 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38200832	Schema change distribution is slowing down replication causing data discrepancy across 2 sites	In a multi-site Policy Control Function (PCF) setup, where site 1 (policy1) was completed a PCF application upgrade that included a schema upgrade, and site 2 (policy3) had fallen behind in replication, resulting in data discrepancies. **Doc Impact**: There is no doc impact.	2	25.1.200
37942052	Replication for Site2 and Site3 went down temporarily during the upgrade of CNDB Site1	When ndbmysql-2 and ndbmysqld-3 pods restarted at the same time during an upgrade in a NDB (MySQL Cluster) setup, it lead to data inconsistency. **Doc Impact**: There is no doc impact.	2	24.2.5
37978500	Incorrect key file for table 'SmPolicyAssociation'; try to repair it	The Incorrect key file for table error was encountered for specific tables like Smservice and common configuration tables. It is recommended to always reopen the table with the missing index. **Doc Impact**: There is no doc impact.	2	23.4.6

Table 4-4 (Cont.) cnDBTier 25.1.103 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37668951	The information_schema and table schema is seen to be inconsistent when policy upgrade was performed	During the 2-site policy upgrade, there was an issue with the schema inconsistency, specifically related to the addition of a new column mode and an index in the table occnp_policyds.pdssubscriber. **Doc Impact**: There is no doc impact.	2	25.1.200
38245044	Documentation should mention which site to be sourced in dbtremovesite	Updated the cnDBTier documentation for `dbtremovesite` to specify which site should be used as the source. **Doc impact**: Updated the "Removing cnDBTier Cluster" section to specify which site should be used as the source when using dbtremovesite script. For more information, see Oracle Communication Cloud Native Core, cnDBTier User Guide.	4	25.1.200

ⓘ **Note**

Resolved bugs from 23.4.7, 24.2.4, and 24.3.1 have been forward ported to release 25.1.103.

Release 25.1.102

Table 4-5 cnDBTier 25.1.102 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38065663	Table entry mismatch over a 2-site 6-channel ASM setup having pod/ container pre-fix	In a two site, six-channel ASM setup, having pod/ container prefix, the multi channel sqllist was not empty and `ignoredb` and `dodb` databases were updated wrongly in the `my.cnf` file. There was a mismatch in tables & entries across the sites. **Doc Impact**: There is no doc impact.	2	25.1.200
38088870	Georeplication was halted in 25.1.200 with 3 channel, replication, Shutdown task and checksum validation tasks were getting halted occasionally	In a three channel replication setup, during the georeplication process the shutdown task threads were occasionally getting stuck in the `db-replication-svc` service. **Doc Impact**: There is no doc impact.	2	25.1.200
37842445	dbtreplmgr script unable to stop replica on HTTPS and TLS enabled setup	In a 4-site, HTTPS and TLS enabled, backup encryption and password encryption enabled setup, when the `dbtreplmgr` script was run to gracefully stop the replication, the replication did not stop and exited with an error. This was due to the hardcoded HTTP parameter in the script. **Doc Impact**: There is no doc impact.	2	24.2.5

Table 4-5 (Cont.) cnDBTier 25.1.102 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38197150	Horizontal data pod scaling failed using dbtscale_ndbmtd_pods script and exited with 'Create Nodegroup FAILED" error	In a four site, ASM enabled, backup encrypted and password encrypted setup, the horizontal data pod scaling failed while using the dbtscale_ndbmtd_pods script and exited with 'Create Nodegroup FAILED" error. Users must wait for the new ndbmtd pods to start and assigned with the "no nodegroup" state before creating the node groups. **Doc Impact**: There is no doc impact.	2	25.1.102
38197150	Retry repartitioning of the tables if any data node is down or backup is in progress	While scaling the ndbmtd pods, repartitioning of the tables was unsuccessful. The `dbt_reorg_table_partition` script must be rerun until the tables are repartitioned successfully if any data node is down or backup is in progress. **Doc Impact**: There is no doc impact.	2	25.1.102

Table 4-5 (Cont.) cnDBTier 25.1.102 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37911174	Doc Changes: Stopping cnDBTier Georeplication Between Sites caused replication outage between all sites	While performing the steps given in the cnDBTier User Guide to stop the cnDBTier while performing georeplication between the sites, was causing replication outage. **Doc Impact**: The "Starting or Stopping cnDBTier Georeplication Service" section was updated to include the following step: • Run the following command to stop the replication service switchover in cnDBTier with respect to siteName: `$ curl -X PUT http://$IP:$PORT/ocdbtier/georeplication/switchover/stop/sitename/{siteName}` For example, run the following command to stop the replication service switchover in cnDBTier with	2	24.2.2

Table 4-5 (Cont.) cnDBTier 25.1.102 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release

		respect to cluster1:
		`$ curl -X PUT http://$IP:$PORT/ocdbtier/georeplication/switchover/stop/sitename/cluster1`
		Sample output:
		`{ "replicationSwitchOver":"stop" }`
		For more information about how to start or stop cnDBTier Georeplication service, see *Oracle Communications Cloud Native Core cnDBTier Installation, Upgrade, and Fault Recovery Guide.*		

38204318	Site removal script dbtremovesite is failing with error of script version mismatch on CNDB v25.1.102	While running the `dbtremovesite` site removal script, the script was failing due to the version mismatch. **Doc impact**: There is no doc impact.	2	25.1.102

Table 4-5 (Cont.) cnDBTier 25.1.102 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38161643	cnDBTier upgrade from 23.4.7 to 25.1.101 failed	cnDBTier upgrade from version 23.4.7 to version 25.1.101 (which was having Webscale version 1.3) was failing because the `kubectl exec` commands did not explicitly specify the container name in Pre/Post upgrade scripts. **Doc Impact**: There is no doc impact.	3	25.1.100
37952176	The metric `db_tier_ndb_backup_in_progress` temporarily shows a value of 1 when a data pod is deleted, even though no backup is actually running on the system	Even though no backup was running on the cnDBTier setup, when a data pod was deleted, the metric `db_tier_ndb_backup_in_progress` temporarily reports a value of 1. **Doc Impact**: There is no doc impact.	3	25.1.100
38077565	Single Stack IPv6 upgrade from 25.1.101 to 25.1.200 pre-upgrade-hooks logs report IPv6 not enabled. Setting LOOPBACK_IP to '127.0.0.1'	In a four site, single-channel cnDBTier setup with IPv6 enabled, when upgrading cnDBTier 25.1.101 to 25.1.200, the pre-upgrade hook incorrectly reported "IPv6 not enabled". **Doc Impact**: There is no doc impact.	3	25.1.200

Table 4-5 (Cont.) cnDBTier 25.1.102 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37943375	The `dbtscale_vertical_pvc` script doesn't throw any error when wrong charts are provided to the script	The `dbtscale_vertical_pvc` script did not throw an error when wrong charts are provided to the script. The `dbtscale_vertical_pvc` script did not validate the chart version. **Doc Impact**: There is no doc impact.	3	25.1.200
38077638	Helm upgrade from 25.1.101 to 25.1.200 reporting TDE secret changed though it was not altered	While upgrading the helm version from 25.1.101 to 25.1.200, in a four site, single-channel, IPv6 enabled setup, the post-upgrade hooks log reported that TDE secret was changed though it was not altered, however `EncryptedFileSystem` was updated in the values.yaml file that resulted in `ndbmtd` pods to restart with `--initial` option. **Doc Impact**: Added the EncryptedFileSystem flag in the "Rolling Back cnDBTier" section in *Oracle Communication Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*	3	25.1.200

Table 4-5 (Cont.) cnDBTier 25.1.102 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38144181	Add the additional replication error numbers, 1091 and 1826 to the list of replication errors and remove the error number 1094 from the list	Added the following new error numbers to the list of replication errors: • 1091 (Can't DROP – column/key doesn't exist) • 1826 (Duplicate foreign key constraint name) Removed the error "1094 - Unknown command" from the list. **Doc Impact**: There is no doc impact.	3	23.4.2
38151238	Observed "ERROR 1296: Got error 4009 'Cluster Failure'" during GRR	In a four site, 3-channel, backup encryption enabled cnDBTier setup, during georeplication recovery process the "Cluster Failure" error was observed. This error occurred while running the `dbtrecover` script during the MONITOR_PARALLEL_BACKUP_TRANSFER and MONITOR_PARALLEL_BACKUP_RESTORE phases. **Doc Impact**: There is no doc impact.	4	25.1.200

Table 4-5 (Cont.) cnDBTier 25.1.102 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37980727	Clarification Required for modifying the https/tls secrets	The section "Certificates to Establish TLS Between Georeplication Sites" in cnDBTier Installation Guide for updating the secrets, did not specify to "Patch" the secret instead of recreating it when the certificate expires or when there is a change in the root CA. The cnDBTier User Guide was updated to add a step to modify SSL/TLS Certificates using the Patch Command Instead of deleting. **Doc Impact**: Updated the section "Certificates to Establish TLS Between Georeplication Sites" to patch the secrets instead of recreating them while establishing TLS between georeplication sites in *Oracle Communication Cloud Native Core, cnDBTier User Guide*.	4	24.2.1

Note

Resolved bugs from 23.4.7, 24.2.4, and 24.3.1 have been forward ported to release 25.1.102.

Release 25.1.101

Table 4-6 cnDBTier 25.1.101 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37807135	`dbtscale_ndbmtd_pods` was not working in release 24.2.5	`dbtscale_ndbmtd_pods` was failing in single-site setup of 24.2.5 as the labels were not present in stateful sets (STS). **Doc Impact**: There is no doc impact.	2	24.2.5
37753846	Vertical scaling of PVC failed while using `dbtscale_vertical_pvc` script	During vertical scaling of Persistent Volume Claim (PVC), the `dbtscale_vertical_pvc` script was failing, because *DBTIER_RELEASE_NAME* was not configured. **Doc Impact**: There is no doc impact.	3	24.2.4
37839960	The `cmp` command was not found in container for which `ndbmtd` pods always perform restart with `--initial` flag	Even when MySQL NDB parameters were not changed, `ndbmtd` pods were restarting with `--initial` flag, because of which the time taken to restart the data nodes had increased. **Doc Impact**: There is no doc impact.	3	25.1.100
37855078	Geo Redundancy Replication was not working in IPv6-enabled cnDBTier deployment	During database replication service deployment, when IPv6 address is configured in the `remotesiteip` configuration, Georedundant Replication (GRR) was not working. **Doc Impact**: There is no doc impact.	3	25.1.100
37789389	`dbtscale_vertical_pvc` script did not work if `ndbdisksize` was in decimal format	`dbtscale_vertical_pvc` script was failing, if `ndbdisksize` value was in decimal format. **Doc Impact**: There is no doc impact.	3	25.1.100

Table 4-6 (Cont.) cnDBTier 25.1.101 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37909755	Documentation required proper release number to be updated for TDE handling with `--initial` flag	In the "Rolling Back cnDBTier" section, the existing NDB parameters list did not provide the TDE parameter that is required to restart the `ndbmtd` pods with `--initial` flag. **Doc Impact**: There is no doc impact.	3	25.1.100

> **Note**
>
> Resolved bugs from 23.4.7, 24.2.4, and 24.3.1 have been forward ported to release 25.1.101.

Table 4-7 cnDBTier 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37468403	Cluster Failure observed in PCF microservices	Schema synchronization issue in MySQL caused cluster failures in PCF microservices. **Doc Impact**: There is no doc impact.	1	23.4.4
37177542	Correct the value of binlogpurgetimer	The default value of binlogpurgetimer was incorrect in the `custom_values.yaml` file. **Doc Impact**: There is no doc impact.	2	24.3.0
37191116	PCF DBTIER 24.2.1 Install - Error with template	Helm chart template issues caused cnDBTier installation to fail on Helm 3.6.x. **Doc Impact**: There is no doc impact.	2	24.2.1
37217585	Incorrect key file for table errors following DBTier GRR	The dbtrecover script did not have an option to restart the SQL pods after performing a georeplication recovery. **Doc Impact**: There is no doc impact.	2	23.4.4

Table 4-7 (Cont.) cnDBTier 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
36615339	cndb ndbmtd-3 pod for site1 and site2 are going into crashloopback after rollback form 24.3.0rc2 to 24.1.1	ndbmtd pods went into the *crashloopback* state after a rollback. **Doc Impact**: There is no doc impact.	2	24.1.0
37077361	Issue being observed in monitoring metrics on 24.3.0; ASM disabled; network policy enabled	DB monitor service had issues with monitoring and fetcing metrics. The following optimizations were performed to resolve this issue: • Thread Pool Management is optimized to resolve issues with metric fetching. • Metric fetching is optimized to prevent multiple database calls for simultaneous requests. **Doc Impact**: There is no doc impact.	2	24.3.0
37214770	Standby replication channel went into FAILED state and didn't recover after restarting one management Dell switch	When adding a site, the system did not insert all records to the DBTIER_INITIAL_BINLOG_POSITION table after scaling ndbmysqld pods. **Doc Impact**: There is no doc impact.	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. **Doc Impact**: There is no doc impact.	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. **Doc Impact**: There is no doc impact.	2	24.3.0
37163647	SR recovery issues	Issues were observed during system file maintenance and recovery. **Doc Impact**: There is no doc impact.	2	24.2.1

Table 4-7 (Cont.) cnDBTier 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37294880	dbtrecover script requires hardening to prevent it from using another version's dbtrecover library files	The `dbtrecover` script used dbtrecover library files from other cnDBTier versions. **Doc Impact**: There is no doc impact.	3	23.4.5
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. **Doc Impact**: Notes are added to *Oracle Communications Cloud Native Core, cnDBTier User Guide* and *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide* to state that the namespace names used in the documents are samples and they must be replaced with the actual namespace name. For more information about the notes, see *Oracle Communications Cloud Native Core, cnDBTier User Guide* and *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*.	3	23.3.1
37101586	Procedure to update vertical scaling for mgm pod should be documented	*Oracle Communications Cloud Native Core, cnDBTier User Guide* didn't include the procedure to scale the management pods vertically. **Doc Impact**: The procedure to vertically scale the management pods is added to *Oracle Communications Cloud Native Core, cnDBTier User Guide*. For more information about this procedure, see *Oracle Communication, Cloud Native Core, cnDBTier User Guide*.	3	24.2.0

Table 4-7 (Cont.) cnDBTier 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37175416	Missing Alerts for NDBAPPMYSQLD or NDBMYSQLD	*Oracle Communications Cloud Native Core, cnDBTier User Guide* did not state that `HIGH_CPU` alerts are specific to data nodes. **Doc Impact**: `HIGH_CPU` alert description in the user guide is updated to include this detail. For more information on this alert, see *Oracle Communications Cloud Native Core, cnDBTier User Guide*.	3	23.4.4
37271956	JVM Matrics glitch in Between Execution for Certain Duration	Database monitor service was unable to fetch JVM metrics intermittently. **Doc Impact**: There is no doc impact.	3	24.3.0
37270980	pvc monitor metrics missed on EIR setup	PVC metrics were not supported in cnDBTier 25.1.100, however cnDBTier did not have an option to disable PVC metrics. **Doc Impact**: There is no doc impact.	3	24.3.0
37359397	occndbtier-24.3.0 db-monitor-svc is reporting multiple error logs with Non GR site	Database monitor service reported multiple error logs when there were no ndbmysqld pods in the cluster. **Doc Impact**: There is no doc impact.	3	24.3.0
37091194	DBTier 24.2.1 RestFuzz scan results flagged 500 (1) Response codes	cnDBTier RestFuzz scan displayed 500 error code for the get@/db-tier/purge/epoch/serverids/{serverIds} API. **Doc Impact**: There is no doc impact.	3	24.2.1
37202609	During DBTier upgrade from 24.2.1 to 24.3.0-rc.2 patching of statefulset.apps/ndbappmysqld is skipped due to kyverno validation failed and later not retried from post-upgrade job	cnDBTier did not retry the updateStrategy patch failures during cnDBTier upgrade. **Doc Impact**: There is no doc impact.	3	24.3.0

Table 4-7 (Cont.) cnDBTier 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37242453	DR failing at state VALIDATERESOURCES and logs do display the reason to the failure	Replication service logs did not capture information about georeplication recovery failures that occurred during the DR_STATE_VALIDATE_RESOURCES state. **Doc Impact**: There is no doc impact.	3	24.3.0
37253044	CNDB OSO Alert file is not appling in OSO 24.3.0 due to the improper structure of the MYSQL_NDB_CLUSTER_DISCONNECT Alert summary and description	cnDBTier OSO alert file was not compatible with OSO due to discrepancies in the `MYSQL_NDB_CLUSTER_DISCONNECT` alert summary and description. **Doc Impact**: There is no doc impact.	3	24.3.0
37273003	Missing metric data on policy SM setup	Metric data were missed intermittently in Policy cnDBTier setup. **Doc Impact**: There is no doc impact.	3	24.3.0
37272556	Error "Removed Meter" observed in db-monitor-svc pod logs of 24.3.0.0.0-rc.8 during EIR traffic run	Meters were not added back after they were removed from the DB monitor service, which was the expected behavious. **Doc Impact**: There is no doc impact.	3	24.3.0
37277299	lost Metrics data/information due to frequent prometheus calls	Metric data was lost due to frequent Prometheous calls. To resolve this issue, the metrics fetching logic in the DB monitor service is optiomized to prevent multiple database calls. **Doc Impact**: There is no doc impact.	3	24.3.0
37281889	The MIB format of dbTier is not compatible with OCCNE MIB definition.	The Management Information Base (MIB) format of cnDBTier was not compatible with the MIB definition in CNE. **Doc Impact**: There is no doc impact.	3	24.3.0

Table 4-7 (Cont.) cnDBTier 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37078075	cnDBtier "Thread pool did not stop" errors log message	cnDBTier logs had the following unnecessary error message which had to be removed: "Thread pool did not stop". **Doc Impact**: There is no doc impact.	3	22.4.2
37058248	DB Tier metrics are missing for some times from the db-monitor-svc	cnDBTier metrics were missing from the DB monitor service as the system was unable to fetch the metrics from the database. **Doc Impact**: There is no doc impact.	3	24.2.0
37106462	DR not failing at VALIDATERESOURCES when bad site has insufficient CPU	Georeplication recovery did not fail during the VALIDATERESOURCES stage when the failed site did not have sufficient CPU resource. **Doc Impact**: There is no doc impact.	3	24.3.0
37143214	All states of DR not displayed when DR triggered via dbtrecover	cnDBTier didn't display all states of georeplication recovery when the georeplication recovery was triggered using the dbtrecover script. **Doc Impact**: There is no doc impact.	3	24.3.0
37288140	DBTier image versions not updated properly in umbrella values.yaml file for 24.2.2 and 24.3.0 DBTier charts	cnDBTier image versions were incorrect in the `custom_values.yaml` file. **Doc Impact**: There is no doc impact.	3	24.3.0
37278381	DR is stuck and continuously retrying backup due to space issue in ndbmtd backup pvc	Fault recovery got stuck and the system tried to take backup continuously even when there was no space available in the ndbmtd backup PVC. **Doc Impact**: There is no doc impact.	3	24.3.0

Table 4-7 (Cont.) cnDBTier 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37352523	Cndb tier 23.4 Helm chart does not pass Helm Strict Linting	Duplicate labels were generated for ndbmysqldsvc. As a result, users were unable to deploy cnDBTier Helm charts. **Doc Impact**: There is no doc impact.	3	23.4.4
36142511	Heartbeat status returns 502 error code when accessed via CNDB sub-menu GUI and REST API for NRF	cnDBTier heart beat status API returned "502 Bad Gateway" response code in the ASM environment. **Doc Impact**: There is no doc impact.	3	23.4.0
37404406	DBTier 24.2.1 helm rollback from TLS to non-TLS same version not dropping TLS	Rollback from a TLS enabled version to a non-TLS version failed as the documentation procedure was not followed correctly. **Doc Impact**: There is no doc impact.	3	24.2.1
37365660	cnDBtier 24.2.2 restore database from backup is not restoring the data completely	The `cndbtier_restore.sh` script did not restore the data completely. **Doc Impact**: There is no doc impact.	3	24.2.2
37601066	cnDBTier:24.2.x:snmp MIB Complain from SNMP server	cnDBTier Simple Network Management Protocol (SNMP) MIB file did not support appending .1 in the OID value. **Doc Impact**: There is no doc impact.	3	24.2.0
37663827	cnDbTier 23.4.7 remote server private keys _permission issue	Permission issues were observed in the remote servers when private keys were set with the permission value of 600. **Doc Impact**: There is no doc impact.	3	23.4.6
37649201	Upgrade failed with error serviceaccount "mysql-cluster-upgrade-serviceaccount" not found	cnDBTier upgrade failed with the 'serviceaccount "mysql-cluster-upgrade-serviceaccount" not found' error, even though the service account existed. **Doc Impact**: There is no doc impact.	3	24.2.2

Table 4-7 (Cont.) cnDBTier 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37270980	PVC monitor metrics missed on EIR setup	cnDBTier did not fetch the metrics continuously when running the traffic on the EIR setup. Instead, there was a break or the metric was omitted on Prometheus. **Doc Impact**: There is no doc impact.	3	24.3.0
37049002	Document cache/realtime time api details in DBtier user guide	cnDBTier API documentation didn't state whether the APIs provides real time or cached data. **Doc Impact**: There is no doc impact.	4	23.4.6
37196445	Documentation error in vertical scaling of ndbmgmd procedure	The procedure to scale ndbmgmd pods vertically was incorrect in the user guide. **Doc Impact**: There is no doc impact.	4	24.3.0
37252269	DR error log not clear for VALIDATERESOURCE state	Fault recovery error log did not provide clear information about the VALIDATERESOURCE state. **Doc Impact**: There is no doc impact.	4	24.3.0
37275946	Hikari connection pool warn message observed in db-monitor-svc logs	Hikari connection pool warning messages were observed in DB monitor service and DB replication service. **Doc Impact**: There is no doc impact.	4	24.3.0
37272259	mysql-cluster-replication-svc logs continuous print of "SSLEngineImpl.java:825| Closing outbound of SSLEngine"	Duplicate SSL messages were observed in replication service logs. **Doc Impact**: There is no doc impact.	4	24.3.0
37144276	DBTier 24.2.1 Network policies - Incorrect pod selector for ndbmysqld	Incorrect pod selector was observed for ndbmysqld pods when network policy was enabled. **Doc Impact**: There is no doc impact.	4	24.2.1

Table 4-7 (Cont.) cnDBTier 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37401291	DBTier User Guide Needs update for BACKUP_SIZE_GROWTH alarm from 23.1.0	The backup size limit after which the `BACKUP_SIZE_GROWTH` alert is triggered was incorrectly mentioned as 5% instead of 20% in the *Oracle Communications Cloud Native Core, cnDBTier User Guide*. **Doc Impact**: There is no doc impact.	4	23.1.0
37550094	In Installation Guide at traffic Segregation with CNLB, mention to change siteport 80 to 8080	CNLB traffic segregation documentation did not contain information about the site port numbers. **Doc Impact**: There is no doc impact.	4	24.3.0

> **Note**
>
> Resolved bugs from 23.4.7, 24.2.4, and 24.3.1 have been forward ported to release 25.1.100.

4.2.4 CNE Resolved Bugs

Release 25.1.101

Table 4-8 CNE 25.1.101 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37854450	CNE Version 25.1.100 fails when issued 'kubectl delete pod' command	While deleting a pod, when 'kubectl delete pod' command was issued, CNE installation failed intermittently. This was caused by the delay in Kyverno API response. **Doc Impact**: There is no doc impact.	2	25.1.100

Table 4-8 (Cont.) CNE 25.1.101 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37869655	CNE Version 25.1.100 fails when issued 'kubectl delete pod' command	In some environments, while trying to delete a pod, deletion command failed due to the delay in the Kyverno API response. **Doc Impact**: There is no doc impact.	2	25.1.100
37799030	CNE installation fails due to missing Velero images	CNE installation failed due to missing Velero build from the source images. **Doc Impact**: There is no doc impact.	3	25.1.100
37842711	CNE installation fails in OL9	In the latest Oracle Linux 9 release, partitions were created differently. However, CNE `cloud_growpart` tasks required specific configuration. This resulted in bastions not having enough space to handle all their dependencies and configuration files leading to CNE installation failure. **Doc Impact**: There is no doc impact.	4	25.1.100

Release 25.1.100

Table 4-9 CNE 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37161841	OCCNE 23.4.1 (LBVM patch 23.4.6) : Security groups are removed from the ports during switchover.	The Load Balancer Controller (`lb-controller`) failed to perform a LBVM switchover when OpenStack compute node hosting the ACTIVE LBVM was shut down. **Doc Impact**: There is no doc impact.	3	• 23.4.1 • 24.3.0 • 24.1.1

Table 4-9 (Cont.) CNE 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36874451	CNE 24.1.0 (Vmware) - OCCNE lb-controller pods stops processing service events or producing logs	The Load Balancer Controller (`lb-controller`) pod was stuck and did not function after getting an exception in the logs. **Doc Impact**: There is no doc impact.	3	24.1.0
37239612	24.2.1 VMware missing egress NAT rules on LBVM	Load Balancer Controller (`lb-controller`) did not install SNAT rules for egress communication. **Doc Impact**: There is no doc impact.	3	24.2.1
37040679	vCNE opnstack upgrade failure with Local DNS enabled due to missing auto plugin config	Upgrade from 23.4.4 failed at the Common Service Upgrade stage due to loss of communication between the cluster and the OpenStack Cloud. This issue was traced back to the Local DNS, which was responsible for OpenStack FQDN resolution. **Doc Impact**: There is no doc impact.	3	24.1.1
37213561	Alerting rules deleted after CNE upgrade	The alerting rules were deleted from NFs after a CNE upgrade. **Doc Impact**: There is no doc impact.	3	24.2.0
37176194	CNE 24.1.1 - Bastion recovery appears to have reset local repo secret, leading to certificate issues	After performing the recovery procedure, Kubernetes reported errors while creating or restarting pods. **Doc Impact**: There is no doc impact.	3	24.1.1

Table 4-9 (Cont.) CNE 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36946610	Repeated OPENSEARCH_DOWN alarms in Prometheus.	`OPENSEARCH_DOWN` alert was triggered with critical severity even when the shards health was yellow (moderate) due to the alert expression. **Doc Impact**: There is no doc impact.	3	23.4.4

> **Note**
>
> Resolved bugs from 24.2.4 and 24.3.2 have been forward ported to Release 25.1.100.

OSO Resolved Bugs

Release 25.1.103

Table 4-10 OSO 25.1.103 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38062402	VNFD has bug double quotes are not correctly defined.	VNFD files had issues. The double quotes were not correctly defined in the files. **Doc Impact**: There is no doc impact.	3	25.1.101
38058360	serverFiles parameter is missing OSO PROM YAML file	The `serverFiles` attribute was missing in `ocoso_csar_25_1_103_0_0_0_prom_custom_values.yaml` file for OSO prometheus. This attribute is used to onboard targets for scraping in prometheus configuration. **Doc Impact**: There is no doc impact.	3	25.1.101

Release 25.1.102

Table 4-11 OSO 25.1.102 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38028960	unknown field "minReadySeconds" install failure in alert manager	Customer used Webscale 1.3 as an underlying platform, which had Kubernetes v1.20. It is required that all Oracle software should be compatible with Webscale 1.3. **Doc Impact**: There is no document impact.	3	25.1.101
37978275	VNFD was expected to reflect two VNF components but only references a single deployment Helm chart	VNFD files in CSAR package were referenced to a single deployment Helm chart instead of two VNF components for Prometheus and Alertmanager charts. **Doc Impact**: Added the following charts and files in the CSAR package: • `prom_deployment_chart` • `alm_deployment_chart` • `prom_values.yaml` • `alm_values.yaml` For more information, see *Oracle Communications Cloud Native Core, Network Repository Function Installation, Upgrade, and Fault Recovery Guide*.	3	25.1.100

Release 25.101

Table 4-12 OSO 25.1.101 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37978275	VNFD was expected to reflect two VNF components but only references a single deployment Helm chart	VNFD files in CSAR package were referenced to a single deployment Helm chart instead of two VNF components for Prometheus and Alertmanager charts. **Doc Impact**: Added the following charts and files in the CSAR package: • `prom_deployment_chart` • `alm_deployment_chart` • `prom_values.yaml` • `alm_values.yaml` For more information, see *Oracle Communications Cloud Native Core, Network Repository Function Installation, Upgrade, and Fault Recovery Guide*.	3	25.1.100

Release 25.1.100

There are no resolved bugs in this release.

4.2.5 NRF Resolved Bugs

Release 25.1.100

Table 4-13 NRF 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37293753	OCNRF 24.2.2: "enableNrfCacheDataService" setting is exposed in custom values yaml file	The `enableNrfCacheDataService` parameter was exposed in the `custom_values.yaml` file and allowed the users to enable or disable the microservice. This parameter should be enabled by default and should not be configurable by the users. **Doc Impact:** `enableNrfCacheDataService` parameter is removed from the Global Parameter section. For more information, see *Oracle Communications Cloud Native Core, Network Repository Function Installation, Upgrade, and Fault Recovery Guide*.	3	24.2.2

Table 4-13 (Cont.) NRF 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37188594	NRF doesn't accept Header 'accept:application/3gppHal+json'	NRF supported only "application/json" media type for GET nf-instances API. Hence, it returned 406 - Not Acceptable error for all other media types than "application/json". "application/3gppHal+json" media type was added to the supported media type list for GET nf-instances API. **Doc Impact:** There is no doc impact.	4	24.1.0

Table 4-13 (Cont.) NRF 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37014400	slfDiscoveredCandidateList is empty when nrfArtisan receives error response from Discovery ms	During NFDiscovery and NRFArtisan microservice internal communication, if the `slfCandidatesList` fetched from NFDiscovery was null, NRFArtisan sent the null value towards NRFConfiguration microservice. There was no impact as NRFConfiguration microservice rejected the requests when NRFArtisan microservice sent request with null value and retained the previous known value. Checks are added if `slfCandidatesList` received from NFDiscovery is not null and sent the request towards NRFConfiguration accordingly. **Doc Impact:** There is no doc impact.	4	24.2.0
34039129	Incorrect response code "408 Request Timeout" in nf Discovery Response from NRF	NRF was returning 408 instead of 500 for SLF query via SCP and SCP sends 504 GatewayTimeout to NRF. **Doc Impact:** There is no doc impact.	4	22.1.0

Table 4-13 (Cont.) NRF 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37535542	OCNRF dashboard not work in OpenShift	NRF dashboard was not working in OpenShift due to issues in e.replace function. **Doc Impact:** There is no doc impact.	3	24.3.0
37633727	ocnrf.forward.nfDiscover.rx.responses is not pegged for alternate NRF retry	`ocnrf_forward_nfDiscover_rx_responses_total` was not getting pegged for alternate NRF retry. **Doc Impact:** There is no doc impact.	3	23.4.0
37597577	OCNRF MIB file used in SNMP server unable to interpret the SNMP traps sent by OCNRF	NRF MIB file used in SNMP server was unable to interpret the SNMP traps sent by NRF. **Doc Impact**: Alerts have been added to interpret the SNMP traps. For more information, see *Oracle Communications Cloud Native Core, Network Repository Function User Guide*.	3	24.2.0

Table 4-13 (Cont.) NRF 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37452088	Removed unused tagContainerName and tagServiceName reference from Overload Configuration	`tagContainerName` and `tagServiceName` variables were removed. **Doc Impact:** `tagContainerName` and `tagServiceName` parameters are removed from the Perf-info Parameter section. For more information, see *Oracle Communications Cloud Native Core, Network Repository Function Installation, Upgrade, and Fault Recovery Guide*.	4	23.3.0
30995300	AdditionalAttributes are getting stored inside nfInfo objects other than the nftype's nfInfo, even when the acceptAdditionalAttributes flag is false	Any additional attribute in the nfInfo object was getting stored. **Doc Impact:** There is no doc impact.	4	1.5.0
37234125	missing namespace-selector for CNCC flows network policy	Applying the default NRF network-policy caused communication issues between CNCC and NRF. **Doc Impact:** There is no doc impact.	3	24.2.0

Table 4-13 (Cont.) NRF 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37633686	ocnrf_nfDiscover_profiles_discovered_total metric is not pegged in forwarding scenarios	Metric values for `ocnrf_nfDiscover_profiles_discovered_total` did not match the nfDiscover requests for a particular nftype. Further debugging showed that the metric pegs are missed in forwarding flows. **Doc Impact:** There is no doc impact.	3	23.4.6
37053943	Custom yaml should mention realtime APIs to monitor DBTier status	NRF `custom_values.yaml` App-Info section was not using cnDBTier Status APIs. **Doc Impact:** `dbStatusUri` parameter is removed from app-info section. For more information, see *Oracle Communications Cloud Native Core, Network Repository Function Installation, Upgrade, and Fault Recovery Guide*.	4	24.2.0
36727455	When cnDBTier is unavailable to NRF, nrfcachedata pods remain UP and nnrf-disc GET returns 200 OK with empty set	When cnDBTier was unavailable to NRF, nrfcachedata pods remained UP and nnrf-discovery service operation returned 200 OK error with empty set rather than 503 Service Unavailable error. **Doc Impact:** There is no doc impact.	3	23.4.0

Table 4-13 (Cont.) NRF 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
35902794	NRF Upgrade is successful with upgrade path from 23.1.x to 23.3.0 even when Infra Validation feature is enabled and minimum upgrade path in custom yaml is 23.2.0	NRF upgrade from 23.1.x to 23.3.0 was successful even when Infra Validation feature was enabled and minimum upgrade path in `custom_values.yaml` was 23.2.0. This upgrade is used as an example. The issue was that the minimum upgrade path value provided in `custom_values.yaml` was not working for the Infra Validation feature. **Doc Impact:** There is no doc impact.	3	23.3.0
36731843	NRF - Error Code ONRF-DIS-DISCSLF-E0403 instead of ONRF-DIS-DISCSLF-E3004 for scenario SLF discovered candidate list is empty.	Problem Details detail attribute contained incorrect App-Error-Id value as ONRF-DIS-DISCSLF-E0403 instead of ONRF-DIS-DISCSLF-E3004 for scenario SLF discovered candidate list is empty in DISCOVERED_SLF_CONFIG_MODE. It should be ONRF-DIS-DISCSLF-E3004. **Doc Impact:** There is no doc impact.	4	24.1.0

Table 4-13 (Cont.) NRF 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
36683249	Incorrect format of detail parameter for Error ONRF-CFG-SCRNRUL-E0007	When error response was sent for NFScreening configuration, the detail attribute in problem details was not in the App-Error-Id format. **Doc Impact:** There is no doc impact.	4	24.1.0
36924403	Incorrect parameter name in invalid-params attribute of Problem Details in the Error Response sent for invalid serving-scope.	The `invalid-params` attribute sent in Problem Details contains the attribute as service-names instead of serving-scope. **Doc Impact:** There is no doc impact.	4	24.2.0
36561654	Incorrect Error code detail format for scenario ONRF-ACC-ACROAM-E0303 NRF peer 3xx response received	The detail attribute format in problem details was incorrect for peer response with status code as 3xx. **Doc Impact:** There is no doc impact.	3	24.1.0
37185716	For NF Profile Retrieval forwarding error scenario in logs, 3gpp-Sbi-Correlation-Info value is getting printed of Request received rather it got from forwarded NRF error response.	For NF Profile Retrieval forwarding error scenario in logs, 3gpp-Sbi-Correlation-Info value was getting printed of Request received rather it got from forwarded NRF error response. **Doc Impact:** There is no doc impact.	3	24.3.0

Table 4-13 (Cont.) NRF 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
35898861	During NRF installation or Upgrade failure after timeout. App-info pod nrf-perf2-ocnrf-app-info-infra-check is running continuously and generating logs.	After there was a failure in NRF installation or upgrade procedure, NRF app-info-infra-check pod was not in completed state but ran continuously and fetched logs. **Doc Impact:** There is no doc impact.	4	23.3.0
35951991	After overriding the same name secrets created from OCCM and performing helm upgrade NRF doesnt use updated certs for TLS Handshake	After overriding the same name secrets created from OCCM and performing Helm upgrade, NRF did not use updated certs for TLS Handshake. **Doc Impact:** There is no doc impact.	3	23.3.0
37813719	NRF is ignoring tai/tac in discovery request	During NF profile processing, if a profile did not match the query parameter, the smfInfoList was set to null and updated in the original profile. As a result, when forwarding, NRF returned an empty response. In this case, NRF treated all profiles as eligible, as profiles without an smfInfoList can be selected for any S-NSSAI, DNN, TAI, and access type. **Doc Impact:** There is no doc impact.	2	23.4.6

Table 4-13 (Cont.) NRF 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37813753	NRF not considering local Subscriptions from local db dip upon 100% packet loss with NRF CacheData Service Microservice pods - Growth feature enabled	NRF did not consider local Subscriptions from local db dip upon 100% packet loss with NRF CacheData Service Microservice pods - Growth feature enabled NRF did not consider local Subscriptions from local db dip upon 100% packet loss with NRF CacheData Service Microservice pods - Growth feature enabled NRF stopped sending the NFStatusNotify service operations and local subscriptions were not considered for generating the NFStatusNotify service operation messages. **Doc Impact:** There is no doc impact.	2	24.2.3
37813766	Multiple 5xx,4xx Error observed during one of the two app-info pod restart continuously for 15 min.	Multiple 5xx, 4xx errors were observed during one of the two app-info pod restart attempts continuously for 15 minutes. **Doc Impact:** There is no doc impact.	3	23.4.6

Table 4-13 (Cont.) NRF 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37813827	NRF is rejecting nfsetid attribute with uppercase value in Registration Request payload	NRF was rejecting service operation with invalid NF Set Id (for example, UDR Registration with upper NFType - UDRSet). Prior to 23.4.0, NRF was allowing both upper and lower case NF Set IDs. However, from 23.4.0, NRF started rejecting service operation having upper case in NF Set ID. Though rejecting service operation is correct if the format is not as per 3GPP, but the behaviour should be controlled by a flag to minimize network impact during upgrade. With this fix, option is provided to enable the 3GPP based behaviour when all of the NFs are complaint with 3GPP defined NF Set ID. **Doc Impact:** There is no doc impact.	3	23.4.0
37813842	Sending of Accept-Encoding header with value as GZIP under configurable flag	Accept-Encoding header was sent with value as gzip under the configurable flag with default value sending the header as before 24.2.2 release. **Doc Impact:** There is no doc impact.	3	24.2.2

Table 4-13 (Cont.) NRF 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37813849	Subscription pod stuck in congested state due to pending message count	Subscription pod was stuck in congested state due to pending message count. **Doc Impact:** There is no doc impact.	2	23.4.6
37813892	Upgrade Failed DB replication	Primary keys were added for NRF backup tables - `NrfSystemOptions_backup` and `NfScreening_backup` for fresh installation. For upgrade cases, primary key is added using MOP. **Doc Impact:** There is no doc impact.	2	23.4.6

ⓘ **Note**

Resolved bugs from 24.3.x have been forward ported to Release 25.1.100.

Table 4-14 NRF ATS 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37334677	One regression feature is not executed through ATS	During ATS regression, the `AccessTokenAuth15_validateTargetNfSetId.feature` was not being executed through the ATS GUI or from the ATS pod.	3	23.4.0
37348692	NRF ATS - PVC Not Attaching to ATS Pod	After the installation of ATS, it was observed that the PVC was not attaching to the ATS pod.	3	24.3.0

Table 4-14 (Cont.) NRF ATS 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37813885	LAB ATS: new feature test cases Config39_SlfRoutesCheck.feature failing	Hardcoded `oncrfPort` value was changed to variable to take values from system.	3	24.2.2

4.2.6 NSSF Resolved Bugs

Release 25.1.100

Table 4-15 NSSF 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37315559	Can the commonCfgServer configuration be removed from the NSSF CV file?	This issue was related to the presence of a redundant configuration section in the NSSF CV file across multiple microservices. Although the comments in the yaml file indicated that this section should not be modified, the support requested its removal from the default `ocnssf_custom_values.yaml` file for future releases. **Doc Impact**: There is no doc impact.	3	24.2.1
37223591	Questions - NSSF 24.1.1	There were queries about NSSF's deregistration behavior under various failure scenarios. The support team requested clarification on handling service failures, including Ingress Gateways, Database status, and NS Subscription or NRF Discovery replicas. **Doc Impact**: There is no doc impact.	3	24.1.1

Table 4-15 (Cont.) NSSF 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36817980	NSSF is sending Tacrangelist in response for NSAvailability procedure but not created in DB (Auth & Rule table) for NSAvailability procedure.	This issue was related to the NSSF sending a `TacRangeList` in the response for the NSAvailability procedure, even though it was not created in the database. The missing entry caused inconsistencies between the response and stored data. The issue was investigated, and the necessary database updates were implemented to ensure consistency. **Doc Impact**: There is no doc impact.	3	24.2.0
37281954	NSSF is not sending notification request retry with max count configured as httpMaxRetries towards AMF for the error response, flag is enabled.	NSSF was not retrying notifications to the AMF as per the configured httpMaxRetries value. The root cause was incorrect mapping of the Helm parameter in the deployment YAML, preventing changes from taking effect. **Doc Impact**: There is no doc impact.	3	24.3.0
37372023	NSSF ATS 24.3.0: ATS installation failed with PV Enabled for VolumeName.	NSSF ATS 24.3.0 installation failed with Persistent Volume enabled due to a volume name validation issue in the Helm charts. The issue was caused by improper handling of PV configurations. The Helm charts were updated to resolve the problem. **Doc Impact**: There is no doc impact.	3	24.3.0

Table 4-15 (Cont.) NSSF 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37225956	User guide needs to be updated with NRF client nfProfileList param details.	The NSSF documents were updated to include details about the NRF client `nfProfileList` parameters. **Doc Impact**: Updated *Network Slice Selection Function Installation, Upgrade, and Fault Recovery Guide* and *Oracle Communications Cloud Native Core, Network Slice Selection Function REST Specification Guide* to document the details of Helm and REST API parameters for `nfProfileList`.	3	24.2.1
36817926	Tailist info is not coming in Availability put response while entry has been created in DB in Auth and Rule table for Availability put procedure for white-listed AMF.	The TAI list information was missing in the Availability PUT response, even though an entry had been created in the database (Auth & Rule table) for an allowed AMF. **Doc Impact**: There is no doc impact.	3	24.2.0
37278862	NSSF is not sending notification retry towards AMF when response for first notification was 404 "subscriber not found" and feature flag is false.	NSSF was not retrying the notification to AMF after receiving a 404 "Subscriber Not Found" response when the feature flag was false, aligning with the behavior mentioned in the *Network Slice Selection Function User Guide*. **Doc Impact**: There is no doc impact.	3	24.3.0
37636625	NSSF:24.3.0: Inconsistencies seen when defining NSS rule with tac.	In NSSF 24.3.0, inconsistencies were observed when defining NSS rules with TAC, as the TAC values were not reflected in responses despite being present in the database. However, when using tacRange, no such issue was found. **Doc Impact**: There is no doc impact.	3	24.3.0

Table 4-15 (Cont.) NSSF 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37717280	NSSF OcnssfOcpmConfigServiceDown Alert - Incorrect Expression.	`OcnssfOcpmConfigServiceDown` alert expression incorrectly used the container dimension in the sum by() function, whereas this metric did not have container as a label. Instead, `app_kubernetes_io_name` should have been used, aligning with other service-down alerts. **Doc Impact**: There is no doc impact.	3	24.2.1
36889943	Traffic moves from site2 to site1, we are getting 404 error code for ns-availability scenarios.	The issue was occurring when traffic was moving from site 2 to site 1 in network slice availability scenarios, resulting in 404 error code. The deployment involved three geographical sites, each handling 3.5K traffic. Despite the replication channel being active, network slice availability data was not synchronizing across all sites as expected, causing request failures. **Doc Impact**: There is no doc impact.	3	24.2.0
37740191	NSSF ATS 25.1.00.rc3, "DNSSRV" feature is randomly failing during ATS run.	DNSSRV feature was failing randomly due to an inconsistency in the `nrfclient_nrf_operative_status` metric validation. The expected count for the service was 1, but the actual count was 0, leading to validation failure. **Doc Impact**: There is no doc impact.	3	24.2.1

Table 4-15 (Cont.) NSSF 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37651423	Subscribe Service Operation error pointing to missing supportedFeatures.	The Network Slice Selection Function was responding with a 400 "BAD_REQUEST" error during the Subscribe Service Operation for the `nnssf-nssaiavailability` service in the customer environment. The error was being caused by a missing supportedFeatures attribute, leading to a NullPointerException during subscription data parsing. According to 3GPP TS 29531, supportedFeatures is a conditional attribute required if any optional features are supported. The error occurred only when duplicate nssai_subscriptions were present in the Database. **Doc Impact**: There is no doc impact.	3	24.3.0
37323951	Prometheus URL comment should be mentioned overload and LCI/OCI feature in NSSF CV file.	The comment for the Prometheus URL in the `ocnssf_custom_values.yaml` file only mentioned its necessity for the Load Control Indicator/Overload Control Indicator feature. However, the URL was also mandatory for the overload feature. Without the correct Prometheus URL, the overload feature was not functioning as expected. **Doc Impact**: There is no doc impact.	4	24.3.0

Table 4-15 (Cont.) NSSF 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37101322	Ephemeral storage of the NSSF deployment is displayed in NSSF Custom Yaml, however it is not displayed when describing the deployment.	The ephemeral storage configuration was present in the `ocnssf_custom_values.yaml` and Helm values but was not reflected when describing the deployment. This was due to missing parameters (logStorage, crictlStorage, and ephemeralStorageLimit) in the custom values file. Without these parameters, the default value was set to 0, disabling ephemeral storage. **Doc Impact**: There is no doc impact.	4	24.3.0
37037110	OCNSSF: averageCpuUtil Parameter missing from Custom Yaml.	The `averageCpuUtil` parameter was missing from the `ocnssf_custom_values.yaml` file, leading to failures in updating the Horizontal Pod Autoscaler (HPA) limits. **Doc Impact**: The details of averageCpuUtil parameter were also updated in the "Customizing NSSF" chapter of the *Network Slice Selection Function Installation, Upgrade, and Fault Recovery Guide.*	4	24.2.0
37270555	Incorrect NF name (NRF instead of NSSF) specified in custom yaml.	Incorrect Network Function name ("NRF" instead of "NSSF") was specified in the `ocnssf_custom_values.yaml` file. This mislabeling appeared in the HTTPS/2.0 configuration comments for the Ingress Gateway. **Doc Impact**: There is no doc impact.	4	24.3.0

Table 4-15 (Cont.) NSSF 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37277288	Statistics name need to be correct in user guide 24.3.0.	The metric name in the Cloud Native Core, Network Slice Selection Function User Guide was incorrectly documented as `ocnssf_nssaiavailability_notification_delete_on_subscription_not_found` instead of `ocnssf_nssaiavailability_notification_delete_on_subscription_not_found_total`, as seen in Grafana. **Doc Impact**: The name of the metric was updated in the *Network Slice Selection Function User Guide* in the relevent sections.	4	24.3.0
37308075	Counter description needs to be documented.	The description for the `Subscription_removed` dimension was missing in the *Network Slice Selection Function User Guide*. **Doc Impact**: The description for the `Subscription_removed` dimension was added in the *Network Slice Selection Function User Guide.*	4	24.3.0

4.2.7 OCCM Resolved Bugs

Release 25.1.100

Table 4-16 OCCM 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37779808	Incorrect alert expression in alert OccmMemoryUsageMinorThreshold	An alert was raised due to incorrect alert expression.	3	24.2.0

Table 4-16 (Cont.) OCCM 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37436671	OCCM 24.3 user guide errors for occm_cert_request_status_total metric and OID 1.3.6.1.4.1.323.5.3.54.1.2.7012	The OID number for `occm_cert_request_status_total` metric was incorrect in the *Oracle Communications Cloud Native Core, Certificate Management User Guide*.	4	24.3.0

> **Note**
>
> Resolved bugs from 24.3.0 have been forward ported to Release 25.1.100.

4.2.8 SCP Resolved Bugs

Release 25.1.100

Table 4-17 SCP 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37490227	SCP generated 429's observed on 24.3.0 GA build even if CPU utilization was at 60%	SCP generated 429 error on 24.3.0 when the CPU utilization was at 60%. **Doc Impact**: There is no doc impact.	2	24.3.0
37662701	SCP worker pod goes into the ContainerStatusUnknown state if the producer's response time exceeds 300 ms	Due to excessive logging, SCP worker pod entered the ContainerStatusUnknown state. This was when the producer's response time exceeded 300 ms and the traffic was running at the rate of 730K MPS. **Doc Impact**: There is no doc impact.	2	24.2.0
37638815	SCP is returning the FQDN in the SCP generated error responses for producers when OCI feature is enabled	When OCI feature was enabled, SCP returned FQDN in the SCP generated error responses for producers. This was resulting in failure of the FT. **Doc Impact**: There is no doc impact.	3	24.2.0

Table 4-17 (Cont.) SCP 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37621268	Circuit breaking Alarm not cleared even traffic reduced to normal state after system recovered from the overload condition	In SCP, circuit breaking alarm remains activated even after traffic was reduced to zero and returned to normal. **Doc Impact**: There is no doc impact.	3	24.2.0
37594916	Observed Null Pointer Exception when SCP is trying to fetch. StaticAlternateRoute configurations	SCP was throwing the Null Pointer exception while trying to fetch the Static Alternate Routing configurations in SCP worker logs. **Doc Impact**: There is no doc impact.	3	24.2.0
37636612	OCSCP 24.2.3: nfTypeExtensionSelfValidation Error for nfTypes encoded with ASN.1 Sequence	When SCP was upgraded from 24.2.1 to 24.2.3, the scp-init pod returned "Incorrect value in Certificate" error in the `nfTypeExtensionSelfValidation` parameter. The NfType value in X509 certificate was '0SCP' instead of 'SCP'. **Doc Impact**: There is no doc impact.	3	24.2.3
37596224	SCP24.2.3: If 3gpp-Sbi-Target-apiRoot sent without port, SCP uses 80 by default for https scheme	For profiles without port, SCP was using port 80 instead of port 443 to generate its tables in https. **Doc Impact**: There is no doc impact.	3	24.2.3
37569488	OCSCP Upgrade from 24.2.2 to 24.2.3 fails during scpc-notification-pre-upgrade job	During scpc-notification-pre-upgrade job, the SCP upgrade from 24.2.2 to 24.2.3 was failing. **Doc Impact**: There is no doc impact.	3	24.2.3

Table 4-17 (Cont.) SCP 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37382873	SCP User Guide typo scp_service dimension	A mismatch in the scp-service dimension was identified. The naming had hyphen in the *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide* and was underscore in Prometheus. **Doc Impact**: The `scp-service` dimension was replaced with `scp_service` in the Metrics section of the *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.	3	24.1.0
37362507	Server Header Behavior	Additional information on SCP's Server Header behavior for Ingress Rate Limiting cases was required to be documented for the Enhanced 5G SBI Message Failure Handling feature. **Doc Impact**: A note related to server header applicable for error responses generated by SCP was added in the Enhanced 5G SBI Message Failure Handling section of the *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.	3	23.4.3
37356571	SCP-audit does hashmap for its own InstanceID results in alert NF_PROFILE_VALIDATION_FAIL	After the retrieval of NF profile for the audit cycle, SCP-Audit was generating a hashmap of its own SCP NF profile instance ID. This led SCP-Audit to send the SCP notification to create an NF rule. **Doc Impact**: There is no doc impact.	3	24.2.1

Table 4-17 (Cont.) SCP 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37190248	SCP Allowing Deletion of Active Routing Config Set Without Reverting Changes	SCP allowed removal of the routing config set without reverting the routing options configuration table on SCP 24.3.0. **Doc Impact**: There is no doc impact.	3	24.3.0
37188165	SCP 23.4.2 : Issue with AR when NFset followed by Static Config w/o Routing Binding header	When a Model-C request was sent "WITHOUT routing-binding header" for a non-existing release towards CHF, it correctly responded with an error "404 NOT FOUND". Here, SCP was responding with "500 Internal error", which was not an expected behavior. **Doc Impact**: There is no doc impact.	3	23.4.2
37175125	requested changes to SCP Capacity and Demand KPIS in SCP provided grafana dashboard	In SCP provided Grafana dashboard, additional dashboard panels were required to be added to provide SCP Capacity and Demand KPIS. **Doc Impact**: There is no doc impact.	3	23.4.3
37274829	SCP 23.4.1 Mediation Drool Rule Code missing semicolon (code and doc issue)	SCP Mediation Drool Rule request code was missing semicolon was identified in the code. The same was documented in the *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*. **Doc Impact**: There is no doc impact.	3	23.4.1
37264009	SCP 24.2.1 - NRF_Configuration DB table is populated incorrectly for nnrf-oauth2 service	In NRF_Configuration DB table, the nnrf-oauth2 service was getting populated incorrectly with the default values from the Helm Charts. **Doc Impact**: There is no doc impact.	3	24.2.1

Table 4-17 (Cont.) SCP 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37256557	SCP : 24.2.1 ATS: S1G4 SCP_DNSSRV_ProducerBasedOverloadControl_P0 110624 failing due to metric mismatch	In the `SCP_DNSSRV_ProducerBasedOverloadControl_P0` feature, the expected and actual counts did not match. **Doc Impact**: There is no doc impact.	3	24.2.1
37256406	latest SCP custom yaml mentioned as " #Default is rel15" but installing on rel16 configuration (rest all config are rel16)	Wrong release number was mentioned for #Default in SCP custom yaml file. **Doc Impact**: There is no doc impact.	3	24.3.0
37213408	SCP percent encoding in Path not working in 24.2.1 release	The RFC percentage encoding in the provided path was not working in 24.2.1 release. **Doc Impact**: There is no doc impact.	3	24.2.1
37200182	Pod Overload control based on pending transactions has gauge metric ocscp_worker_pending_upstream_resp_count left with stale count	It was identified that the Pod Overload control based on pending transactions had stale count set in `ocscp_worker_pending_upstream_resp_count` `gauge` metric.	3	24.3.0
37099264	Observed that 500 "task queue full" metrics is missing in SCP metric ocscp_metric_scp_generated_response_total	It was observed that While testing demo scenarios to simulate overload condition, SCP generated error log with response code as 500. The same was not captured in `ocscp_metric_scp_generated_response_total` metric. However, Egress response rate 500 was pegged. **Doc Impact**: There is no doc impact.	3	24.2.1
37087633	SCP goes into unstable state when traffic goes above 944K MPS	It was observed that whenever the traffic goes beyond 944K MPS, SCP went into unstable state. **Doc Impact**: There is no doc impact.	3	24.2.1

Table 4-17 (Cont.) SCP 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37084277	SCP 2 worker pods restarted on 28K TPS with 49000 msec response delay.	It was observed that, two SCP worker pods were restarting on 28K TPS with 49000 msec response delay. **Doc Impact**: There is no doc impact.	3	24.3.0
36981688	SCP not retrying when srv:maxRoutingAttempts=1 and 503 response generated by SCP.	When the maxRoutingAttempts is set 1 for the nchf-spendinglimitcontrol service name, SCP was unable to connect to CHF and produces 503 Service Unavailable error response. It was observed that the SCP was not even trying to alternate CHFs as it should. **Doc Impact**: There is no doc impact.	3	24.1.0
36977823	Metrics Stats For the SCP Mediation Service is not supported in ATS	It was observed that the mediation service was not supporting pre-fetch and post-fetch stats required to validate the metrics. **Doc Impact**: There is no doc impact.	3	24.2.0
36932681	Helm Charts missing cipherSuites	It was observed that the Helm Charts were missing cipherSuites, due to which SCP worker pod were not active during SCP deployment. **Doc Impact**: There is no doc impact.	3	24.2.0
36928108	ocscp_nf_unhealthy	An obsolete metric ocscp_nf_unhealthy was identified in Prometheus. **Doc Impact**: There is no doc impact.	3	23.4.3
36925908	Scp save mediation trigger points is rejected with missleading/incorrect error when http method is empty	It was identified that there were no validation for Http Methods in Mediation Trigger Points. **Doc Impact**: There is no doc impact.	3	24.2.0

Table 4-17 (Cont.) SCP 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36925392	On recreating SCP secret for scp-worker pod after it's deletion from scp namespace, scp-worker pod is restarting continuously.	It was identified that the scp-worker pod is continuously restarting, while recreating SCP secret for scp-worker pod after deleting it from SCP namespace. **Doc Impact**: There is no doc impact.	3	24.2.0
36340289	SCP 23.3.0 NF Profile Registration failed due to NF_RESOURCE_MAPPINGS table size	It was observed that the NF Profiles (AUSF, UDM) registration were rejected by SCP due to error in creating entries in NF_RESOURCE_MAPPINGS database table. **Doc Impact**: There is no doc impact.	3	23.3.0
37045773	SCP 23.4.3 - Server Header - sideCarProxyStatusCode is mandatory - Bad Request	Configuring the Enable Enhance Server Header behavior was not possible without sidecar Proxy Status Code. **Doc Impact**: There is no doc impact.	3	23.4.3
37037530	Incorrect ocscp_producer_service_instance_id observed in metrics	`Incorrect ocscp_producer_service_instance_id` were getting populated in two of the metrics. **Doc Impact**: There is no doc impact.	3	24.3.0
37193860	429's overload errors observed occasionally on 24.3.0	While running the traffic at the rate of 730K MPS with 200ms deplay applied on SCP, 429's overload error was observed. **Doc Impact**: There is no doc impact.	3	24.3.0
37606298	OCSCP:24.2.1:snmp MIB Complain from SNMP server	SNMP-Notifier was returning incorrect MIB information in the alert trap towards SNMP server to OCCNE. **Doc Impact**: There is no doc impact.	4	24.2.1

Table 4-17 (Cont.) SCP 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37575952	SCP 24.2.1 Warn Log observed for Internal error in SCPC-Notification microservice	While performing SCP health-check, some internal error as WARN logs were observed in SCPC-Notification microservice. **Doc Impact**: There is no doc impact.	4	24.2.1
37466021	SCP should not get out internally added headers (eg x-scp-authority) as part of outgoing request to peer NF	It was observed that the PCAP for egress request SCP was returning internally added headers in the outgoing request to peer NF. **Doc Impact**: There is no doc impact.	4	24.2.0
37367706	Documentation of test results from big tickets to SCP User Guide	It was observed that the *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide* required more information on consumer SCP under InterSCP Routing in the 5G SBI Message Routing section. **Doc Impact**: A note related to producer NF's locality selection was added in the *5G SBI Message Routing* section of the *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.	4	24.3.0
37324506	SCP 24.2.1 : SCP Mediation pods having 2 ERROR messages	Post deployment to SCP 24.2.1, two errors were observed in SCP Mediation pods. **Doc Impact**: There is no doc impact.	4	24.2.1
37190282	NF Registration Throws Incorrect Error Response When Routing Config Set Is Absent	When the routing config set which is being used in routing options configuration is not present, then NF Registration was returning Incorrect Error Response. **Doc Impact**: There is no doc impact.	4	24.3.0

Table 4-17 (Cont.) SCP 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37168856	Threshold values needs to be updated in the alerts yaml as per the dimensioning sheet	It was observed that the threshold values of all alerts in yaml file needed to be updated based on dimensioning sheet. **Doc Impact**: There is no doc impact.	4	24.2.1
37107520	Getting connectionFailed instead of connectionTimeout in error response	In the Error response Enhancement feature, connectionFailed was returned instead of connectionTimeout in error response. **Doc Impact**: There is no doc impact.	4	24.3.0
37051489	Inconsistent useCachedRecordOnError parameter validation: 502 Not Listed in REST API Documentation but allowed	It was observed that the parameter `useCachedRecordOnError` was accepting value 502, which was not documented in the *Oracle Communications Cloud Native Core, Service Communication Proxy REST Specification Guide* as allowed values. **Doc Impact**: The allowed values of the *useCachedRecordOnError* REST API parameter was updated in the *Configuring SCP Features* section of the *Oracle Communications Cloud Native Core, Service Communication Proxy REST Specification Guide*.	4	24.3.0
37043155	Getting ocscp_consumer_nf_type as NA instead of SMF in the metrics	One of the metrics was receiving "NA" instead of "SMF" as response for `ocscp_consumer_nf_type`. **Doc Impact**: There is no doc impact.	4	24.3.0
37037931	Getting status_code as "200 OK" instead of "200" in metrics	One of the metrics was receiving "200 OK" instead of "200" as response for status_code. **Doc Impact**: There is no doc impact.	4	24.3.0

Table 4-17 (Cont.) SCP 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37037823	Getting ocscp_response_code as "200 OK" instead of "200" in metrics	One of the metrics was receiving "200 OK" instead of "200" as response for ocscp_response_code. **Doc Impact**: There is no doc impact.	4	24.3.0
37011971	Incorrect/ambiguous metric name	Two of the metrics had incorrect names and were pegged at nrfproxy/worker when the cache was invalidated on receiving notification from NRF. **Doc Impact**: There is no doc impact.	4	24.3.0
36307322	SCP 22.4 User Guide: Dimensions of the metrics needs to be corrected	It was observed that some of the metrics information needed to be in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*. **Doc Impact**: There is no doc impact.	4	22.4.0

ⓘ **Note**

Resolved bugs from 24.2.3 have been forward ported to Release 25.1.100.

4.2.9 SEPP Resolved Bugs

Release SEPP 25.1.102

Table 4-18 SEPP 25.1.102 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38201407	SEPP mediation use case not mediating HTTP Status Code	The requirement was to mediate the HTTP status code for a response with "400 Bad Request" and convert it to "200 OK". The pn32f microservice sent the "x-original-status" header along with the 400 Bad Request to the mediation layer, which successfully updated the header and returned the response to pn32f. However, pn32f did not update the HTTP status code based on the new "x-original-status" value; instead, it simply appended the new "x-original-status" header without changing the original status code. **Doc Impact**: Added a note about the x-original-status header to the Custom Headers section of 5G SBI Message Mediation Support feature.	3	25.1.100

Release SEPP ATS 25.1.102

Table 4-19 SEPP ATS 25.1.102 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38196990	ATS feature files are failing on ATS release 25.1.200 with Webscale 1.3(k8 1.20)	ATS feature files were failing on ATS Release - 25.1.200. For PSEPP side cases, a Kubernetes service was created to retrieve the `ipFamilies` configuration from the stubserver-1 service. Based on this configuration, a new service was created with the same IP family settings. However, since Kubernetes version 1.20 did not support dual-stack networking, the `ipFamilies` field was not populated in the stubserver-1 service. This resulted in a KeyError when attempting to access `service_yaml['spec']['ipFamilies']`. The code was fixed to work on Kubernetes versions that did not support dual-stack networking. **Doc Impact**: There is no doc impact.	2	25.1.100

> **Note**
>
> Resolved bugs from 24.3.1 have been forward ported to Release 25.1.102.

Release 25.1.101

Table 4-20 SEPP 25.1.101 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38039149	No alerts are generated when the SEPP Services are unavailable.	The SEPP software packages currently do not include 'Service Unavailable' alerts in the Alerts Configuration file for SEPP microservices. The request is to define a critical alert for each microservice. **Doc Impact**: Added the system alerts in the *System Alerts* section of *Oracle Communications Cloud Native Core, Security Edge Protection Proxy User Guide*.	3	25.1.100
38039154	Removal of pre-fixed 0 when negotiated PLMN column is updated in PLMN table .	The leading zero in 3-digit MNCs is removed when the negotiated PLMN state is updated in the PLMN table. The correct PLMN ID will be displayed in the Handshake Status screen **Doc Impact**: There is no doc impact.	3	25.1.100

> ⓘ **Note**
>
> Resolved bugs from 24.3.1 have been forward ported to Release 25.1.101.

Release 25.1.100

Table 4-21 SEPP 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36919451	SEPP_PERF: ocsepp-n32-ingress-gateway restart and call failed observed with error code 500,503,504,408 observed during 42K MPS performance run at 24.2.0-GA with topology Hiding, Cat(0,1,2,3),Overload,Mediation,SOR,RateLimit feature enabled	The ocsepp-n32-ingress-gateway was restarted, and calls failed with error codes 500, 503, 504, and 408 during a 42K MPS performance run at release version 24.2.0 with topology hiding, SCM (Cat0, Cat1, Cat2, and Cat3), Overload, Mediation, SOR, and RateLimiting features enabled. **Doc Impact**: There is no doc impact.	2	24.2.0

37356760	corrupts multipart messages Content-Transfer-Encoding binary	When a multipart message was received at SEPP, the `application/vnd.3gpp.5gnas` part was corrupted by the Egress Gateway.
		The message received at `plmn-ingress` showed:`Content-Transfer-Encoding: binary`
		`c1917b00298080211001000010810600000000083060000000000d00000a00000500001000001100002300002400`
		However, in the Egress Gateway message from `n32egress`, it appeared as:`Content-Transfer-Encoding: binary`
		`efbfbdefbfbd7b0029efbfbdefbfbd211001000010efbfbd0600000000efbfbd0600000000000d00000a00000500001000001100002300002400`
		This indicates that the content was altered during transmission.
		Doc Impact:
		There is no doc impact.
			2	24.2.1

Table 4-21   (Cont.) SEPP 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37731720	Observed 425 errors during SEPP perf run while running pSEPP site down scenario	During a SEPP performance run with fault insertion scenarios, the 425 error occurred on the cSEPP side when the pSEPP was brought up after a full scale-down period. The issue is related to the plmn-egress-gateway rejecting requests due to a DNS resolution failure. The problem was identified as a race condition. When ARS came online after PLMN Egress Gateway, it failed to update the configuration on PLMN Egress Gateway. Consequently, PLMN Egress Gateway continued sending 425 errors, which resulted in total traffic loss. **Doc Impact**: There is no doc impact.	2	24.3.1
37222975	SEPP-ASM-Install/Upgrade: Unable to Install ocsepp-servicemesh with ocsepp-servicemesh-config-24.3.0.tgz Charts Error: INSTALLATION FAILED: Chart.yaml file is missing	The installation failed when using `ocsepp-servicemesh`with the `ocsepp-servicemesh-config-24.3.0.tgz`file. The error message received was: `NSTALLATION FAILED: Chart.yaml file is missing.` **Doc Impact**: There is no doc impact.	3	24.3.0
37134044	SEPP 24_2_0 ,Äì Detailed IP/ Service Flow	A document was required that contained the detailed IP/ service flow for SEPP, which could be referred to during testing. **Doc Impact**: There is no doc impact.	3	24.2.0

Table 4-21 (Cont.) SEPP 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37126321	SEPP 24.2.0 - Network policies helm charts not packaged correctly	The network policy helm charts of SEPP in version 24.2.0 were not packaged correctly, which caused the `helm install` to fail. The current `.tgz` file name was `ocsepp-network-policy-24.2.0.tgz`. When decompressed, the directory was `ocsepp-network-policy-24.2.0`, but the directory should have been `ocsepp-network-policy`. **Doc Impact**: There is no doc impact.	3	24.2.0
36453267	SEPP_PERF: Some discrepancy found at SEPP_24.1.0_rc1 default yaml resource profile and sepp 24.1.0 doc resource profile	Some discrepancies were found between the SEPP 24.1.0 rc1 default YAML resource profile and the documented resource profile. • The `Alternate-Route replica` count was different. • The Gateway replica counts were also different. **Doc Impact**: There is no doc impact.	3	24.1.0
37046531	[SEPP-Perf] SEPP Call failures with 4xx & 5xx Error codes with 24K MPS traffic with message copy	When the Message Copy feature was enabled at both the PLMN-IGW and N32-EGW of SEPP, call failures were observed with 4xx and 5xx error codes. This caused each SEPP site to handle 24K MPS of traffic, with MessageCopy traffic adding another 24K MPS towards OCNADD. After a 12-hour overnight run, around 1.7% of calls were dropped. **Doc Impact**: There is no doc impact.	3	24.2.0

Table 4-21 (Cont.) SEPP 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37234008	SEPP-Install/Upgrade: Error(DBHealthCheck","message":"The connection to the database is active) observed at cn32f microservice after SEPP_24.3.0 fresh installation at NoN-ASM & ASM setup	An error was observed at the `cn32f` microservice after a fresh installation of SEPP 24.3.0 in both NoN-ASM and ASM setups. The error message was: `Error(DBHealthCheck", "message": "The connection to the database is active)` Additionally, an extra log was being printed continuously. **Doc Impact**: There is no doc impact.	3	24.3.0
37187193	SEPP 24.2.0 - Routing to Remote SEPP with TLS disabled using DNS SRV	The DNS SRV section in the *Oracle Communications Cloud Native Core, Security Edge Protection Proxy User Guide* had to be updated with the details. **Doc Impact**: The "Alternate Routing based on the DNS SRV Record for Home Network Functions" section in the Oracle Communications Cloud Native Core, Security Edge Protection Proxy User Guide has been updated. New parameters have been added to the n32-egress-gateway and plmn-egress-gateway sections of the *Oracle Communications Cloud Native Core, Security Edge Protection Proxy Installation, Upgrade, and Fault Recovery Guide*.	3	24.2.0

Table 4-21 (Cont.) SEPP 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37276057	[SEPP] Absence of failure reason in alert SEPPPn32cHandshakeFailureAlert	In the alert section of the *Oracle Communications Cloud Native Core, Security Edge Protection Proxy User Guide*, the SEPPPn32cHandshakeFailureAlert table stated: "The failure reason was present in the alert." However, based on testing, it was found that the `SEPPPn32cHandshakeFailureAlert` did not contain the failure reason. **Doc Impact**: Updated the `SEPPPn32cHandshakeFailureAlert` of *Alert* section of *Oracle Communications Cloud Native Core, Security Edge Protection Proxy User Guide*.	3	24.3.0
36767431	Call failed observed with error code 500,503,504,408 during and n32-ingress-gateway restart with 137-Error code during 56K MPS performance run with Cat3 feature enabled with cache refresh time 120000 at sepp_24.2.0	During a 56K MPS performance run with the Cat-3 feature enabled and a cache refresh time of 120000 at SEPP 24.2.0, the `n32-ingress-gateway` encountered 137 error codes. Calls failed with error codes 500, 503, 504, and 408. **Doc Impact**: There is no doc impact.	3	24.2.0
37410882	SEPP as a Roaming hub is sending PlmnIdList when it is not supposed to send	SEPP as a Roaming hub was sending PlmnIdList in capability-exchange response message even when `n32cHandshakePlmnIdListValidationEnabled` is set to false. **Doc Impact**: There is no doc impact.	3	24.3.1

Table 4-21 (Cont.) SEPP 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release

37527327	False Helm message is observed for rate limiting configmaps after SEPP uninstallation	When SEPP was uninstalled, a false message was observed after the uninstall was completed.
		These resources were kept due to the resource policy:
		`[ConfigMap] egress-ratelimit-map`
		`[ConfigMap] rss-ratelimit-map`
		The release "ocsepp-release" was uninstalled.
		Doc Impact:
		There is no doc impact.
			3	24.3.0

37112128	PLMN List not match with remote PLMN list	When additional PLMNs were sent in the capability-exchange message, which were not supported by the Remote SEPP, the handshake was not successful. **Doc Impact**: There is no doc impact.	3	24.2.0
37520228	SUT installation creates multiple roles, service accounts and rolebindings	The SEPP 24.3.0 SUT installation created multiple roles, service accounts, and rolebindings automatically. The CV file did not have a global parameter for providing the service account name to be used. The requirement was to provide a single service account in the global section of the SEPP CV file so that a single role would be used. **Doc Impact**: There is no doc impact.	3	24.3.0

Table 4-21 (Cont.) SEPP 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37513097	ATS testcase does not use customer specific plmns	The SEPP ATS test cases did not support the use of customer-specific PLMNs, MCC 311 and MNC 480. This caused the network ID and PLMN ID verification-related test cases to fail when the SEPP SUT was deployed with PLMN 311, 480. The requirement was to make the PLMN IDs configurable for ATS. **Doc Impact**: There is no doc impact.	3	24.3.0
36630098	Producer FQDN in the TxRequest metadata copies "port" from api'root in the incoming Rx	The `'producer-fqdn'` header contained the FQDN+port, although it should have only included the FQDN. **Doc Impact**: There is no doc impact.	4	23.4.0
35925855	x-reroute-attempt-count and x-retry-attempt-count header come twice in response when Alternate routing feature is enabled	A message was sent through SBI when the Alternate Routing feature was enabled, and alternate routing (either static or dynamic) was applied to the SBI message, with a duplicate `x-reroute-attempt-count` and `x-retry-attempt-count` headers found in the outgoing message. **Doc Impact**: There is no doc impact.	4	23.3.0
36577846	improper value of InstanceIdentifier in oc_egressgateway_outgoing_tls_connections metric	In the `'oc_egressgateway_outgoing_tls_connections'` metrics, an incorrect value for the `InstanceIdentifier` was observed, which was set to `"UNKNOWN_egressgateway"`. **Doc Impact**: There is no doc impact.	4	24.1.0

Table 4-21 (Cont.) SEPP 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37446555	debug is set to true for app-info in SEPP custom yaml	The redundant entry was removed from `custom-values.yaml` to update the logs of `appinfo`. **Doc Impact**: There is no doc impact.	4	24.3.0
37225506	SEPP 24.2.0: SEPP not sending SNI header in client hello to remote SEPP	The SEPP did not send the SNI header in the client hello to the remote SEPP. The *Oracle Communications Cloud Native Core, Security Edge Protection Proxy User Guide* has to be updated to address the issues. **Doc Impact**: Updated the descriptions of the Remote SEPP IP Address and N32F IP Address parameters in the Remote SEPP section of the *Oracle Communications Cloud Native Core, Security Edge Protection Proxy User Guide*.	4	24.2.0
37482952	oc_ingressgateway_route_overloadcontrol_total Metric Not Visible in Prometheus.	The `oc_ingressgateway_route_overloadcontrol_total` metric was not visible in Prometheus. **Doc Impact**: There is no doc impact.	4	24.3.0

Table 4-21 (Cont.) SEPP 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release

36605719	Warnings being displayed while installing mediation due to k8sResource.container.prefix/ suffix parameter	The following warnings were printed during the installation:
		`helm install -f custom.yaml ocsepp ocsepp/ -nns`
		`coalesce.go:286: warning: cannot overwrite table with non table for ocsepp.k8sResource.container.prefix (map[])`
		`coalesce.go:286: warning: cannot overwrite table with non table for ocsepp.k8sResource.container.suffix (map[])`
		`coalesce.go:286: warning: cannot overwrite table with non table for ocsepp.nf-mediation.global.k8sResource.container.prefix (map[])`
		`coalesce.go:286: warning: cannot overwrite table with non table for ocsepp.nf-mediation.global.k8sResource.container.suffix (map[])`
		These warnings were caused by the parameters suffix and prefix in the mediation charts, which had the value {}. The installation was successful, but the warnings should not have been printed.
		Doc Impact:
		There is no doc impact.
			4	24.1.0

> **Note**
>
> Resolved bugs from 24.3.1 have been forward ported to Release 25.1.100.

4.2.10 UDR Resolved Bugs

Release 25.1.100

Table 4-22 UDR 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37388443	Bulk Import Tool importing custom parameters with "\" character	There was an extra backslash ("\") inserted into the JSON structure of custom parameters for bulk import tool. **Doc Impact:** There is no doc impact.	2	24.2.0
36921424	java.lang.NullPointerException in the error-reason header in response when GET request has invalid user-agent header	When GET request had invalid User Agent Header there was java.lang.NullPointerException in the error-reason header response. **Doc Impact:** There is no doc impact.	3	24.2.0
36381825	Helm chart does not pass Helm Strict Linting	The Helm chart was not passing the Helm strict linting. **Doc Impact:** There is no doc impact.	3	22.3.2
37049563	Customer requesting KPI and dashboard for ASM	A KPI dashboard was requested for Aspen Service Mesh (ASM). **Doc Impact:** There is no doc impact.	3	24.1.0
37320719	GRR PVC need to be updated in 24.3.0 from 8Gi to 66Gi for EIR	Geo Replication Recovery (GRR) Persistent Volume Claim (PVC) was to be updated from 8Gi to 66Gi for Equipment Identity Register (EIR). **Doc Impact:** There is no doc impact.	3	24.3.0

Table 4-22 (Cont.) UDR 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37187864	Optimization of Variable in CNDB Custom values yaml for EIR	Values were incorrect in the CNDB yaml file used for EIR.	3	24.3.0
37301547	Subscriber Export Tool Status in the GUI does not update during export	The CNC Console was not updating the subscriber export tool status. **Doc Impact:** There is no doc impact.	3	24.2.0
37660632	PNR is not generated for Sh interface when DiamGW identify is changed	PNR (Push Notification Request) was not generating for diameter SH when diameter gateway was changed. **Doc Impact:** There is no doc impact.	3	24.2.0
37339535	SLF-ATS 24.3.0: New Features failing due to validation failure exception	SLF ATS new features was failing due to validation failure exception. **Doc Impact:** There is no doc impact.	3	24.3.0
36829292	UserAgent Validation is by default set to true for IGW-PROV after installation if we enable UserAgent Header feature	UserAgent Validation was set to true by default for ingress gateway provisioning are installation. **Doc Impact:** There is no doc impact.	3	24.2.0
37226597	PROVGW - We are not able to see application log level for prov ingress and egress gateway on CNCC GUI	Application Log Level was not visible for provisioning gateway ingress gateway and egress gateway on CNC Console. **Doc Impact:** There is no doc impact.	4	24.3.0

Table 4-22 (Cont.) UDR 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37053924	Custom yaml should mention realtime APIs to monitor DBTier status	Real time APIs was not used in the custom yaml file to monitor cnDBTier status. **Doc Impact:** There is no doc impact.	4	24.2.0
37390366	During 18.2K N36 Performance with real cnPCRF if we restart UDR DIAMGW pods, N36 Traffic is dropped to 0	The N36 traffic was dropping to zero when UDR diamenter gateway pods were restarted during 18.2K N36 performance test with cnPCRF. **Doc Impact:** There is no doc impact.	4	24.2.2
37354405	SLF-Bulk-Import- We need to rename the file expiry parameter from CNCC console	The file expiry parameter was renamed in the CNC Console for Subscriber Bulk Import Configurations. **Doc Impact**: Updated the parameter name to Import File Expiry Time in the *Subscriber Bulk Import Configurations* section of the *Oracle Communications Cloud Native Core, Unified Data Repository User Guide.*	4	24.3.0

Note

Resolved bugs from 24.3.0 have been forward ported to Release 25.1.100.

4.2.11 Common Services Resolved Bugs

4.2.11.1 ATS Resolved Bugs

Release 25.1.100

There are no resolved bugs in this release.

4.2.11.2 ASM Configuration Resolved Bugs

Release 25.1.100

There are no resolved bugs in this release.

4.2.11.3 Alternate Route Service Resolved Bugs

Table 4-23 Alternate Route Service 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
36935315	Implement SA Guidelines for SecurityContext Configuration on GW	Some of the fields and SecurityContext configuration were not done for Gateway Services.	3	24.3.0
37039309	Tcpdump and Ping tools of debug tools is not working in egress gateway debug tools container	Tcpdump and Ping tools of debug tools did not work in Egress Gateway debug tools container.	3	24.3.0

ⓘ **Note**

Resolved bugs from 24.3.x have been forward ported to Release 25.1.100.

4.2.11.4 Egress Gateway Resolved Bugs

Table 4-24 Egress Gateway 25.1.103 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37685576	Flooded with IRC Exception warn messages in EGW	Received the `IllegalReferenceCountException` warn messages in Egress Gateway after editing some values of traffic.sidecar.istio.io/excludeInboundPorts or traffic.sidecar.istio.io/excludeOutboundPorts in the Egress Gateway deployment and SVC.	2	24.2.11
37601685	High CPU when reset streams are triggered	Gateway Services experienced high CPU when reset streams were triggered.	2	24.2.12

Note

Resolved bugs from 24.2.x have been forward ported to Release 25.1.103.

Table 4-25 Egress Gateway 25.1.102 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37480520	After successful update of certificate in NRF k8S by OCCM by recreate process new certificate validity is not used in TLS handshake by NRF GW	After successful update of the certificate in NRF Kubernetes by OCCM (recreation process), the new certificate validity was not used in the TLS handshake by NRF Gateway Services.	2	25.1.100
37009578	SCP Monitoring not happening for subset of configured SCPs	SCP monitoring did not happen for the subset of configured SCPs.	2	23.4.4
37563087	Traffic routing done based on deleted peer/peerset and routes	Traffic routing was done based on the deleted peer or peerset and routes.	2	25.1.100

Note

Resolved bugs from 23.4.x have been forward ported to Release 25.1.102.

Table 4-26 Egress Gateway 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37319725	Update Notify sent towards SMF via EGW, fails at EGW due to NullPointerException followed by a timeout	The Update Notify sent towards SMF through Egress Gateway failed at Egress Gateway due to NullPointerException followed by a timeout.	2	25.1.100
37363928	Handshake failure when SEPP Egress gateway not initiating TLS connection	The handshake failure occurred when SEPP Egress Gateway did not initiate a TLS connection.	2	25.1.100
36935315	Implement SA Guidelines for SecurityContext Configuration on GW	Some of the fields and SecurityContext configuration were not done for Gateway Services.	3	24.3.0
36928822	No error codes observed in the Egress GW Grafana dashboard when FQDN is mis-configured	No error codes were observed in the Egress Gateway Grafana dashboard when FQDN was incorrectly configured.	2	23.4.4
37143723	If peer1 is used as a virtual host, which is not resolved, egress gateway is not routing the request to peer2 , which is host and port. Also, peer health status is empty	When peer 1 was used as a virtual host, which was not resolved, Egress Gateway did not route the request to peer 2, which was a host and port. Also, peer health status was empty.	3	24.2.4
37194307	Egress gateway drops all SEPP traffic after some time on dual stack setup	On a dual stack setup, SEPP traffic was processed, however, the SEPP traffic was blocked after some time due to IllegalStateException on n32-egress-gateway.	3	24.3.1

Table 4-26 (Cont.) Egress Gateway 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37236640	Timeout exception occurred while sending notification request to Notification Server (25.1.0)	Timeout exception occurred while sending Notification requests to the Notification server.	2	23.2.12
36876832	100% CPU and traffic failures observed at EGW	100% CPU and traffic failures were observed at Egress Gateway.	2	23.4.7
36938693	EGW pods getting stuck and not processing any traffic (Policy 24.3.0)	Egress Gateway pods were stuck and could not process any traffic.	2	23.4.8
36950565	Body omitted from request while sending multipart messages	While enhancing SEPP to support multipart messages, it was observed that N32-EGW was sending empty body in the request, but it received the full payload from the CN32F service.	2	24.2.0
36666519	Producer/Consumer FQDN contain ":port" while messageCopy is enabled on GWs	FQDN of producer NF and consumer NF had ":port" while messageCopy was enabled on Gateway Services.	4	23.4.0
36987637	Egress gateway jetty client not able to handle HTTP2 zero size header table	Egress Gateway Jetty client was unable to handle the HTTP2 zero size header table.	2	24.1.5
35927069	Entry updated in DNS Server is not getting reflected while checking the healthStatus in Egress Gateway	The entry updated in DNS Server did not appear while checking the healthStatus in Egress Gateway.	3	23.3.3
36305260	Egress gateway is adding duplicate headers in response [Alternate routing use case}	Egress Gateway added multiple duplicate headers, x-reroute-attempt-count and x-retry-attempt-count, in responses.	3	24.1.0

Table 4-26 (Cont.) Egress Gateway 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37039309	Tcpdump and Ping tools of debug tools is not working in egress gateway debug tools container	Tcpdump and Ping tools of debug tools did not work in Egress Gateway debug tools container.	3	24.3.0
37148443	Egress gateway not accepting IPv6 address in the configuration	In the Roaming partner profile, when IPv6 address was provided in the Remote SEPP IP address, Egress Gateway did not accept IPv6 address in the configuration.	3	24.3.1
37236640	Timeout exception occurred while sending notification request to Notification Server (25.1.0)	Timeout exception occurred while sending Notification requests to the Notification server.	2	23.2.12

> **Note**
>
> Resolved bugs from 24.1.x have been forward ported to Release 25.1.100.

4.2.11.5 Ingress Gateway Resolved Bugs

Table 4-27 Ingress Gateway 25.1.103 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37601685	High CPU when reset streams are triggered	Gateway Services experienced high CPU when reset streams were triggered.	2	24.2.12

> **Note**
>
> Resolved bugs from 24.2.x have been forward ported to Release 25.1.103.

Table 4-28 Ingress Gateway 25.1.102 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37744851	Installation is failing with POP25 validation failrure even though POP25 feature is disabled	The Ingress Gateway Helm installation failed with a POP25 validation failure.	3	25.1.101
37333191	oc_ingressgateway_http_responses_total metrics are not updated when call is rejected by ratelimiting	The `oc_ingressgateway_http_responses_total` metric was not updated when the call was rejected by rate limiting.	3	25.1.100
37365106	401 unauthorized metric not updated in "oc_ingressgateway_http_responses_total"	The oc_ingressgateway_http_responses_total metric was not updated when the call was rejected by rate limiting with ASM enabled.	3	25.1.100
37369197	Error reason for Pod protection by rate limiting is not updated for default error profile.	The error reason for the Pod Protection using Rate Limiting feature was not updated for the default error profile.	4	25.1.100
37403771	NRF upgrade failed with igw post upgrade hooks in error state	NRF upgrade failed with Ingress Gateway postupgrade hooks in the error state.	2	23.4.10
37417212	Rest Configuration is success for ERROR Profile which is not defined in values file	The REST configuration was successful for ERROR Profile which was not defined in the values file.	4	25.1.100
37416293	Fill rate is allowing decimal value during helm but same is rejecting in REST configuration	The Fill rate allowed the decimal value during the Helm configuration, however, the same was rejected in the REST configuration.	4	25.1.100

Table 4-28   (Cont.) Ingress Gateway 25.1.102 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37359902	Success percentage drops to 47-52% during in-service upgrade/ rollback of IGW from 24.3.3 to 25.1.0 and vice-versa	Success percentage reduced to 47-52% during the in-service upgrade or rollback of Ingress gateway from 24.3.3 to 25.1.0 and conversely.	2	25.1.100
37480520	After successful update of certificate in NRF k8S by OCCM by recreate process new certificate validity is not used in TLS handshake by NRF GW	After successful update of the certificate in NRF Kubernetes by OCCM (recreation process), the new certificate validity was not used in the TLS handshake by NRF Gateway Services.	2	25.1.100
37563087	Traffic routing done based on deleted peer/peerset and routes	Traffic routing was done based on the deleted peer or peerset and routes.	2	25.1.100

ⓘ **Note**

Resolved bugs from 23.4.x have been forward ported to Release 25.1.102.

Table 4-29   Ingress Gateway 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
36935315	Implement SA Guidelines for SecurityContext Configuration on GW	Some of the fields and SecurityContext configuration were not done for Gateway Services.	3	24.3.0
36932086	mcore-ingress-gateway pod keeps increasing until the pod is restarted	The mcore-ingress-gateway pod continued to increase until the pod restarted.	2	23.4.4
36672146	3gpp-sbi-lci header is not included in response for signalling requests	The 3gpp-sbi-lci header was not included in the response for signaling requests.	3	24.2.1

Table 4-29 (Cont.) Ingress Gateway 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
36915822	IGW sends requests to NRF backend services when they are in NotReady (0/1) state	Ingress Gateway sent requests to NRF discovery service pods when the pods were in the NotReady(0/1) state.	3	23.4.3
37032005	IGW is timing out with 408 request intermittently	Ingress Gateway was timing out for certain messages, and in such cases, logs were observed in Ingress Gateway.	3	24.3.0
36882493	NullPointerException From IGW for GET pending-req-count	NullPointerException was observed in Ingress Gateway for the GET pending-req-count.	2	23.4.6
36950565	Body omitted from request while sending multipart messages	While enhancing SEPP to support multipart messages, it was observed that N32-EGW was sending empty body in the request, but it received the full payload from the CN32F service.	2	24.2.0
37039309	Tcpdump and Ping tools of debug tools is not working in egress gateway debug tools container	Tcpdump and Ping tools of debug tools did not work in Egress Gateway debug tools container.	3	24.3.0

ⓘ **Note**

Resolved bugs from 23.4.x have been forward ported to Release 25.1.100.

4.2.11.6 Common Configuration Service Resolved Bugs

Release 25.1.100

There are no resolved bugs in this release.

4.2.11.7 Helm Test Resolved Bugs

Release 25.1.100

There are no resolved bugs in this release.

4.2.11.8 App-Info Resolved Bugs

Release 25.1.100

There are no resolved bugs in this release.

4.2.11.9 Mediation Resolved Bugs

Table 4-30 Mediation 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37313319	If Mediation Rule name have Special characters in It,The Rule get saved with Encoded value of the special character	If the Mediation rule name had special characters, the rule was getting saved with encoded value of the special character.	3	24.3.0
37274829	Mediation Drool Rule Code missing semicolon (code and doc issue)	Semicolon was missing in Mediation Drool Rule	3	23.4.1

4.2.11.10 NRF-Client Resolved Bugs

Table 4-31 NRF-Client 25.1.100 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
36730314	[AM_UE Performance]upgrade fails from PCF 24.1.0_GA to 24.2.0_rc7 " Error creating bean with name 'hookService' defined in URL"	While upgrading NRF-client some how there are multiple records in the common config hook db, this generates issues while completing the hook process. Until now the workaround was to manually delete the duplicate records.	2	24.2.0
37746681	NRF-Client Sends continous PUT/ PATCH requests to NRF when UDR is in SUSPENDED state	When the NF changes from running to not running, NRF-client enters into an endless cycle of PUT and PATCH request part of the hearbeat process. This overloads with many requests.	2	25.1.100

4.2.11.11 Perf-Info Resolved Bugs

Release 25.1.100

There are no resolved bugs in this release.

4.2.11.12 Debug Tool Resolved Bugs

Release 25.1.100

There are no resolved bugs in this release.

4.3 Known Bug List

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

4.3.1 BSF Known Bugs

Release 25.1.100

There are no known bugs in this release. Known bugs from 24.3.0 have been forward ported to Release 25.1.100.

4.3.2 CNC Console Known Bugs

Release 25.1.100

There are no known bugs in this release.

4.3.3 cnDBTier Known Bugs

Release 25.1.103

Table 4-32 cnDBTier 25.1.103 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
38199454	DB Entries on Site-1 and Site-2 are not in sync after doing an in service upgrade from 24.2.6 to 25.1.200 on a 2 site GR setup	After performing an in-service upgrade from version 24.2.6 to 25.1.200 on a 2-site Geo-Replication (GR) setup, database entries between Site-1 and Site-2 are not in sync.	Replication delay is observed. **Workaround**: Perform the following steps: 1. Complete the DBTier software upgrade. All the DB Tier pods should be upgraded to the new DBTier version. 2. Perform rolling restart of ndbappmysqld and ndbmysqld stateful sets.	2	24.2.6

Release 25.1.102

Table 4-33 cnDBTier 25.1.102 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
38199454	DB Entries on Site-1 and Site-2 are not in sync after doing an in service upgrade from 24.2.6 to 25.1.200 on a 2 site GR setup	After performing an in-service upgrade from version 24.2.6 to 25.1.200 on a 2-site Geo-Replication (GR) setup, database entries between Site-1 and Site-2 are not in sync.	Replication delay is observed. **Workaround**: Perform the following steps: 1. Complete the DBTier software upgrade. All the DB Tier pods should be upgraded to the new DBTier version. 2. Perform rolling restart of ndbappmysqld and ndbmysqld stateful sets.	2	24.2.6
38220013	dbtrecover Script is affecting db-monitor-svc	After running georeplication recovery (GRR), the db-mon-svc service intermittently enters a deadlock state, leading to unresponsiveness of both its db-mon-svc REST API and metrics scraping. This condition persists until the service is restarted.	Intermittently after running GRR, db-mon-svc has deadlock threads. Db-mon-svc API and metric scraping are not working until it gets restarted. **Workaround**: Restart the DB Monitor service after georeplication recovery is completed	3	25.1.100

Release 25.1.101

Table 4-34 cnDBTier 25.1.101 Known Bugs

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

Release 25.1.100

Table 4-35 cnDBTier 25.1.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37839960	The ndbmtd pods restart with "initial" option, due to which the restart time of the pod increases	During a single or multisite deployment, when the cluster is upgraded with configuration changes, the ndbmtd pods restart with -- initial option. This is because the cmp command in the ol9 docker container is removed. This leads to the increased pod restart time.	The issue increases the upgrade time because the ndbmtd pods take more time to restart. **Workaround**: Perform upgrade or rollback of cnDBTier without service account instead of automated upgrade or rollback using the service account.	3	25.1.100

4.3.4 CNE Known Bugs

Release 25.1.101

Table 4-36 CNE 25.1.101 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36740199	bmCNE installation on X9-2 servers fail	Preboot execution environment 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 23.3.1 or older version on X9-2 servers.	2	23.4.0

Release 25.1.100

Table 4-37 CNE 25.1.100 Known Bugs

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

Table 4-37 (Cont.) CNE 25.1.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37799030	OCCNE images_25.1.100.tar missing velero images	CNE 25.1.100 doesn't have the Velero images in the images tar file. This issue can lead to install and upgrade failures.	This issue can cause CNE 25.1.100 installation and upgrade failures. **Workaround**: Download Velero images from the internet. Additionally, perform the following steps after provisioning the registry with the necessary images while configuring the container image registry. For more information, see the "Configuring Container Image Registry" section (Step 1) in *Oracle Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide*. - Run the following commands to set a common environment: **Provision the registry with the**	2	25.1.100

Table 4-37 (Cont.) CNE 25.1.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release

			necessary Velero images
			`$ CENTRAL_REPO=<central-repo-name>`
			`$ CENTRAL_REPO_REGISTRY_PORT=<central-repo-registry-port>`
			`$ OCCNE_VERSION=<OCCNE version>`
			`$ OCCNE_CLUSTER=<cluster-name>`
			`$ OCCNE_vCNE=<openstack, oci,`		

Table 4-37 (Cont.) CNE 25.1.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release

			`vmware, or`
			`do`
			`not define`
			`if`
			`Bare-Metal>`
			`$`
			`if`
			`[ -x`
			`"$(command -v podman)"`
			`];`
			`then`
			`OCCNE_CONTAI`		

Table 4-37 (Cont.) CNE 25.1.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release

			`NER_ENGINE=`
			`'podman'`
			`else`
			`OCCNE_CONTAINER_ENGINE=`
			`'docker'`
			`fi`
			- Create a text file with Velero images:
			`$`
			`cat`
			`<<EOF >> velero`		

Table 4-37 (Cont.) CNE 25.1.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
			_images.txt docker.io /velero/velero :v1.13.2 docker.io /velero/velero_plugin_for_aws :1.9.2 docker.io /velero/velero_plugi		

Table 4-37 (Cont.) CNE 25.1.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release

			`n_for_csi`
			`:0.7.1`
			`EOF`
			- Load Velero images on Central Repo Registry:
			`$`
			`for`
			`IMAGE`
			`in`
			`$(`
			`cat`
			`velero_images.txt);`
			`do`
			`TAGGED_IMAGE`		

Table 4-37 (Cont.) CNE 25.1.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
			_NAME= $ {IMAGE / docker .io\ / velero \ // occne/ } $ {OCCNE _CONTA INER_E NGINE} image pull $ {IMAGE } $ {OCCNE _CONTA INER_E		

Table 4-37   (Cont.) CNE 25.1.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
			NGINE} image tag ${IMAGE} ${CENTRAL_REPO}:${CENTRAL_REPO_REGISTRY_PORT}/${TAGGED_IMAGE_NAME} ${OCCNE_CONTAINER_ENGINE} image push ${CENTRAL_REPO}:${CENTRAL_REPO_REGISTRY_PORT}/${TAGGED_IMAG		

Table 4-37 (Cont.) CNE 25.1.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release

			`E_NAME}`
			`${OCCNE_CONTAINER_ENGINE} image`
			`rm`
			`${IMAGE}`
			`${CENTRAL_REPO}:${CENTRAL_REPO_REGISTRY_PORT}/${TAGGED_IMAGE_NAME}`
			`done`		

OSO Known Bugs

Release 25.1.103

There are no known bugs in this release.

Release 25.1.102

There are no known bugs in this release.

Release 25.1.101

There are no known bugs in this release.

Release 25.1.100

There are no known bugs in this release.

4.3.5 NRF Known Bugs

Release 25.1.100

Table 4-38 NRF 25.1.100 Known Bugs

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

Table 4-38 (Cont.) NRF 25.1.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37760595	While validating the Sustenance bug OCNRF-9417 - Discovery query results in incorrect match with preferred-locality=US%2bEast	NRF is returning NFProfile ordered at first position with locality matching with space (i.e. US East) while query contains + (i.e. US+East).	NFProfiles in response may be ordered with space first then followed by other localities **Workaround**: Locality attribute shall not have space or plus as special characters. Or if query have %252B as encoded character then NFProfile with + will match i.e. US+East.	3	24.2.4

Table 4-38 (Cont.) NRF 25.1.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37784967	DiscoveryResultLoadThreshold feature, discovery response contains Profile having load value(30) greater then DiscoveryResultLoadThreshold (20)	For DiscoveryResultLoadThreshold Feature, Use-Case Background:- 1. service-names query parameter is present in NFDiscover service operation query 2. Filtered NFProfile has only one NFService. 3. Load is not present at NFservice level	This only happens for DiscoveryResultLoadThreshold feature, when service-names query parameter is present in NFDiscover service operation query and filtered NFProfile has only one NFService and that NFService don't have load value present. **Workaround**: DiscoveryResultLoadThreshold feature value is 0. So, feature is not applied.	3	24.2.4

Table 4-38 (Cont.) NRF 25.1.100 Known Bugs

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

Table 4-38 (Cont.) NRF 25.1.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37788289	Discovery query results in Empty Profile when discovery query is forwarded due to AMF profile is Suspended and Empty response received from Forwarded NRF	When Discovery query is received for target nf type AMF and guami query parameters, and the matching profiles are in SUSPENDED state, it is expected that the SUSPENDED profiles are returned in the discovery response when emptylist feature is enabled.However, due to this bug, the suspended profiles are not returned.	Consumer NFs will not receive SUSPENDED AMFs when they try to discover AMF with guami. **Workaround**: There is no workaround available. If forwarding is enabled, then it is possible that the response will contain AMF profiles from the other segment.	3	24.2.4
37797310	NFRegistration logs some attributes are showing wrong data	NFRegistration logs some attributes are showing wrong data.	NFRegistration microservice some of the attributes logs may have wrong data. **Workaround**: There is no workaround available.	4	24.2.4

Table 4-38 (Cont.) NRF 25.1.100 Known Bugs

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

4.3.6 NSSF Known Bugs

Release 25.1.100

Table 4-39   NSSF 25.1.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37048499	GR replication is breaking post rollback to of CNDB 24.2.1-rc.4	The cnDBTier replication mechanism is experiencing performance degradation during rollbacks under high transaction volumes, leading to potential transaction ordering inconsistencies and constraint failures on the secondary site. Additionally, any binlog instruction failure is disrupting the replication channel. For the Network Service Selection Function (NSSF), the NsAvailability functionality is encountering a replication channel break when rolling back an upgrade from 24.2.x to 24.3.x if an availability delete and an availability update are occurring within a few seconds.	NSSF's Availability (NsAvailability) functionality may experience a replication channel break during the rollback of an upgrade from 24.2.x to 24.3.x if an availability delete and an availability update occur within a short time frame of a few seconds. **Workaround:** If the replication channel breaks, it can be recovered by following the replication channel recovery procedure outlined in the section 7.4.7.1 – Resolving Georeplication Failure Between cnDBTier Clusters in a Two-Site Replication in the *Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*.	24.3.0	2

Table 4-39 (Cont.) NSSF 25.1.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37776049	Dynamic log level updating Using CNCC for various micro services for NSSF. "LogDiscarding" Option is coming while fetching configured log level via REST but in CNCC while configured that option is not present	NsConfig Log level is not updated at runtime.	There is no impact on traffic; however, debugging becomes difficult if the NsConfig service log level needs to be changed at runtime. **Workaround:** Helm parameter can be used to change the log level of NsConfig. It can be modified as needed.	25.1.100	3
37773632	[10.5K TPS] when we are deleting all CNDB pods, ns-selection 2 pods have stuck in a 1/2 state.	When all pods of cnDBTier are deleted then NSSF NsSelection pods are getting stuck.	There is minimal impact on traffic when cnDBTier recovers. However, if all cnDBTier pods are deleted, NsSelection pods may not distribute traffic properly, leading to pods getting stuck. **Workaround:** Delete the stuck pods. Newly spawned pods will be able to take traffic.	25.1.100	3
37763453	Error code 500, instead 4XX, when NSSF receives duplicated incorrect Authorization	Ingress Gateway is not responding with error when Auth token is incorrect.	There is no traffic loss. **Workaround:** There is no workaround available.	24.3.0	3

Table 4-39 (Cont.) NSSF 25.1.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37762864	[10.5K TPS] nrf-client discovery and management pod has restarted when all CNDB pod faults using chaos-mesh	When cnDBTier pod is forcefully kept in a stuck state, NRF-client pods enter a restart state.	There is no impact on traffic when the cnDBTier pods are recovered. **Workaround:** There is no workaround available.	25.1.100	3
37731732	Autopopulation with 3NRFs: Even though candidate AMF doesn't have same plmn as amfset it is storing in database and is getting resolved when amf resolution is called	NSSF is autopopulating AMF candidates from NRFs into the Database (DB) even when the candidate AMF does not belong to the same PLMN as the AMF set.	There is no traffic loss. **Workaround:** There is no workaround available.	25.1.100	3
37684563	[10.5K Traffic—without Replication Break] While 7K burst traffic to site1, NSSF reduced the success rate by 3.528% with 500 and 503 error code and then recovered it	Intermittent loss of traffic occurs when traffic is moved from one site to another.	Minimal traffic loss, with approximately 3.5% of traffic lost for a few seconds before recovering. **Workaround:** There is no workaround available.	25.1.100	3
37684124	[10.5K Traffic] while adding the empty frame in all requests, NSSF rejected the ns-selection traffic, dropping 0.045% with a 503 error code	Intermittent traffic loss occurs when traffic is moved from one site to another.	There is minimal traffic loss of approximately 3.5%, which occurs for a few seconds before the traffic recovers. **Workaround:** There is no workaround available.	25.1.100	3

Table 4-39 (Cont.) NSSF 25.1.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37681032	NSSF 24.2.1: Missing Edit Option for nsconfig Logging Levels in CNCC GUI	When an empty packet is forcefully added to traffic (negative scenario), 0.045% of traffic is discarded with error code 503.	There is minimal traffic loss of 0.045%, occurring only in an error scenario. **Workaround:** There is no workaround available.	24.2.1	3
37639879	oauth failure is not coming in oc_ingressgateway_http_responses_total metrics	There is an Incorrect metric pegging for *oc_ingress_http_response_total* in the OAuth failure scenario.	There is no impact on the traffic. **Workaround:** There is no workaround available.	25.1.100	3
37623199	If an accept header is invalid, NSSF should not send a notification to AMF. it should send 4xx instead of 500 responses to the nsssai-auth PUT and DELETE configuration.	NSSF is performing database (DB) operations and triggering notifications to the AMF even when an invalid Accept header was present in nsssai-auth PUT and DELETE requests.	There is no impact on the traffic. **Workaround:** There is no workaround available.	25.1.100	3
37606284	With DNS SRV feature enabled for selection of NRF, NSSF fails to establish connection with NRF	When tested with three NRF instances configured across different sites, using geo-redundant ASM-based deployment, NSSF failed to establish a connection with the NRF when DNS SRV-based discovery was enabled.	There is no impact on the traffic. **Workaround:** There is no workaround available.	25.1.100	3

Table 4-39 (Cont.) NSSF 25.1.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37591102	OCNSSF:24.2.x:snmp MIB Complain from SNMP server	SNMP traps are not being raised due to an issue with the MIB file.	There is no impact on the traffic. **Workaround:** Updated MIB file with scope set to shared.	24.2.0	3
37216832	[9K TPS Success] [1K TPS Slice not configured in DB] NSSF is sending the success responses for slice which has not configured in database and failure response of slice which has configured in database for pdu session establishment request.	In an error scenario test where 9,000 error messages are sent, NSSF is incorrectly responding with success for 0.4% of the messages.	There is minimal impact on the traffic. **Workaround:** There is no workaround available.	24.3.0	3
37184196	3-site GR setup ASM and Oauth Enabled : 10.5K TPS Traffic on SITE1 : during restoration of site (post Failover for 18 hours), new NsAvailability PUT is not syncing to site which is recovered	Intermittently, after replication recovery, data is not synchronized, leading to error responses for a limited duration.	There is minimal impact on the traffic. **Workaround:** There is no workaround available.	24.3.0	3
37136539	[dnsSrvEnabled: false] [peer Health monitoring: disabled] NSSF is not sending the notification towards peer2 host if peer1 is down	When DnsServices is disabled and static routes are used, notifications are not rerouted when the primary peer is down.	There is a loss of notification in a specific case when static routing is used. **Workaround:** Enable DnsServices and use virtual FQDNs.	24.2.1	3
37136248	If dnsSrvEnabled is set to false and peer1 is used as a virtual host, the egress gateway will not sending the notification to peer2 host and peer health status is empty	Health check status processing has an issue at the Egress Gateway, causing requests to be forwarded to an unhealthy peer.	There is no traffic loss, as the message is retried and eventually reaches the correct node. **Workaround:** There is no workaround available.	24.2.1	3

Table 4-39 (Cont.) NSSF 25.1.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37099843	Upgrade 3 Site GR Setup, while upgrading NSSF and CNDB, we observed that the Ns-availability success rate dropped 0.07%, 0.77%, and 1.19%, respectively, for each site, and we got 500, 503, and 403, 408 error codes.	During an in-service upgrade, 0.25% to 1% of messages are being responded to with error codes.	During an upgrade, 0.25% to 1% of messages are lost. The impact is low as this occurs only during upgrade or rollback when pods are starting. After the upgrade, the behavior returns to normal. **Workaround:** There is no workaround available.	24.3.0	3
36734417	NSSF 2 Site GR :IN service solution Upgrade : 1.25K TPS : traffic loss of 0.259% and 0.027% at Site 1 and Site 2 during the NSSF upgrades, with latency of roughly 1.43 seconds and 886 ms.	During an in-service upgrade, 0.25% of messages are being responded to with error codes.	During an upgrade, 0.25% of messages are lost. The impact is low as this occurs only during upgrade or rollback when the pods are starting. **Workaround:** There is no workaround available.	24.2.0	3
36662054	NSSF-CNCC: Ingress pod: Discard Policy mapping configured without mandatory param	The CNCC GUI does not validate the Discard Policy mapping configuration.	There is no impact on the traffic. **Workaround:** The operator can configure the Discard Policy mapping with the correct value.	24.1.0	3

Table 4-39 (Cont.) NSSF 25.1.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36552026	KeyId, certName, kSecretName, and certAlgorithm invalid values are not validating in the oauthvalidator configuration.	Invalid values for KeyId, certName, kSecretName, and certAlgorithm are not being validated in the OAuthValidator configuration.	There is no impact on the traffic. **Workaround:** While configuring the OAuthValidator, the operator must ensure proper values are used.	24.1.0	3
36285762	After restarting the NSselection pod, NSSF is transmitting an inaccurate NF Level value to ZERO percentage.	After restarting the NsSelection pod, NSSF is transmitting an inaccurate NF Level value.	There is no impact on the traffic. **Workaround:** NA	23.4.0	3
36265745	NSSF is only sending NF-Instanse/NF-Service load level information for multiple AMF Get Requests	When multiple AMF are sending requests to NsSelection microservice, then for some requests, only NF-Instance scope LCI headers are received or only NF-Service scope LCI headers are received.	There is no impact on the traffic. **Workaround:** There is no workaround available.	23.4.0	3
35971708	while pod protection is disabled, OcnssfIngressGatewayPodResourceStateMajor alert is not clear and resource metric is not updating to -1	When the Pod Protection feature is disabled, the previous alerts are not getting cleared.	There is no impact on the traffic. **Workaround:** There is no workaround available.	23.3.0	3
35922130	Key Validation is missing for Ingress Gateway pod protection parameter name configuration	The Ingress Gateway REST API configuration is missing validations for the POD Protection feature.	There is no impact, as the operator can configure correct values as mentioned in the guide. **Workaround:** Configure NSSF with the correct values as per the REST API guide.	23.3.0	3

Table 4-39 (Cont.) NSSF 25.1.100 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 is missing validations.	The Pod Protection configuration is accepting invalid values. **Workaround:** The operator must ensure that the configured values should align with the guidelines provided in the documentation.	23.3.0	3
35888411	Wrong peer health status is coming "DNS SRV Based Selection of SCP in NSSF"	NSSF is not showing as unhealthy for a non-existent SCP. If peerConfiguration is set with the first peer as a non-existent SCP and the second peer as a virtual host, the peerHealth status incorrectly shows peer1 as healthy, despite it being non-existent.	There is no impact on the traffic. A non-responsive SCP is not considered for status. As a result, no status is displayed. **Workaround:** There is no workaround available.	23.3.0	3
35860137	In Policy Mapping Configuration in Ingress Gateway, For the samplingPeriod parameter, max value of parameter validation should be necessary.	Rest API for configuration of ocpolicymapping has missing validations.	There is no impact on the traffic. **Workaround:** The operator must ensure the configuration values should align with the guidelines provided in the documentation.	23.3.0	3
37622760	NSSF should send 415 responses to ns-selection and ns-availability requests if their content type is invalid.	NSSF responds with the 405 error instead of the 406 error when an invalid header value for Content-Type is provided.	There is no impact on the traffic. **Workaround:** NA	25.1.100	4

Table 4-39 (Cont.) NSSF 25.1.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37617910	If ns-selection and ns-availability are invalid Accept Header, NSSF should not send 404 responses of UnSubscribe and subscription patch request. it should be 406 error code and "detail":"No acceptable".	NSSF responds with the 405 error instead of the 406 error when an invalid header value for Access-Type is provided.	There is no impact on the traffic. **Workaround:** There is no workaround available.	25.1.100	4
37612743	If URLs for ns-selection and ns-availability are invalid, NSSF should return a 400 error code and title with INVALID_URI.	NSSF responds with the 405 error instead of the 400 error when an invalid URI is provided.	There is no impact on the traffic. **Workaround:** There is no workaround available.	25.1.100	4
37606772	3-site GR setup ASM and Oauth Enabled: 15K TPS Traffic on SITE1 : we observed the 503 SERVICE_UNAVAILABLE error code	In an overload scenario, when 155% of traffic is sent, NSSF intermittently responds with the 503 error.	There is minimal impact on traffic in an overload scenario. **Workaround:** There is no workaround available.	25.1.100	4
37592343	Subscription Patch should be a part of Availability Sub Success (2xx) % panel in Grafana Dashboard	The Grafana dashboard does not include the subscription patch in the status of NsAvailability Pod state computation.	There is no impact on the traffic. **Workaround:** There is no workaround available.	25.1.100	4
36881883	In Grafana, Service Status Panel is showing more than 100% for Ns-Selection and Ns-Avaliability Data	The Grafana dashboard is showing more than 100% success, which is incorrect.	There is no impact on the traffic. **Workaround:** There is no workaround available.	24.2.0	4
36653494	If KID is missing in access token, NSSF should not send "Kid missing" instead of "kid configured does not match with the one present in the token"	The error response text is not in line with the expected format.	There is no impact on the traffic. **Workaround:** There is no workaround available.	24.1.0	4

Table 4-39 (Cont.) NSSF 25.1.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35986423	Both Ingress Gateway pod protection and overload feature enabled, NSSF is not clearing the overload alerts when overload feature disabled in runtime.	Alerts for Overload Control are not getting cleared when the feature is disabled.	There is no impact on the traffic. **Workaround:** There is no workaround available.	23.3.0	4
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 the pod is in a DOC (Dead or Clogged) condition. The issue is that once an alert is raised, it does not subside even after the condition is updated.	There is no impact on the traffic, as NSSF manages the condition. However, the alert subsides only when there is a change in state. **Workaround:** There is no workaround available.	23.3.0	4
35855377	The abatementValue less than onsetValue should be validated by NSSF in the Overload Level Threshold Configuration.	The Ingress Gateway REST API configuration is missing validations for the Overload feature.	There is no impact on the traffic, as the operator can configure the Overload feature with the correct values as mentioned in the REST API guide. **Workaround:** Configure the Overload feature with the correct values as per the REST API guide.	23.3.0	4

4.3.7 OCCM Known Bugs

Release 25.1.100

There are no known bugs in this release.

4.3.8 SCP Known Bugs

Release 25.1.100

Table 4-40 SCP 25.1.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37721950	Getting IP instead of FQDN in peerscpfqdn dimension of SCPUnhealthyPeerSCPDetected Alert	SCP receives IP addresses instead of FQDNs in the peerscpfqdn dimension of the SCPUnhealthyPeerSCPDetected alert.	IP address is displayed instead of FQDN in the alert. This is the correct IP address of SCP. **Workaround**: There is no workaround available.	3	25.1.100
37721565	If, SCP received request message with 3gpp-Sbi-Client-Credentials header with x5u - X.509 URL , then SCP should passthrough without CCA validation and should not reject the request message.	When SCP receives a request message with the 3gpp-Sbi-Client-Credentials header with x5u - X.509 URL, SCP should pass through without CCA validation and without rejecting the request message.	If SCP receives the request with the 3gpp-Sbi-Client-Credentials header with x5u - X.509 URL, the request is rejected. **Workaround**: Use the 3gpp-Sbi-Client-Credentials header with x5c instead of x5u in the request.	3	25.1.100
37713112	Not responding to consumer in case of incorrect LCI headers	SCP does not respond to the consumer NF when SCP receives incorrect LCI headers from the producer NF.	SCP does not process the response with incorrect LCI header format.	3	25.1.100
37622431	Audit failures observed during overload situation when traffic is operating at maximum rated capacity and surpasses the pod limits by 50%.	When traffic is operating at maximum rated capacity and exceeds the pod limits by 50%, audit failures are observed while SCP is in the overload condition.	In overload conditions, SCP-Worker pod protection mechanism discards some of the internally generated NRF audit requests. **Workaround**:	3	25.1.100

Table 4-40 (Cont.) SCP 25.1.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37575057	Duplicate Routing when producer responses with location header in 3xx cases	SCP performs duplicate routing when the producer NF responds with the location header in 3xx cases.	SCP will send requests to producer NF again if the producer NF in redirect URL and alternate routing rules are the same. **Workaround**: There is no workaround available.	3	25.1.100
37572287	Multiple worker pods restart observed in the event of cache pods get into a restart state when traffic is running at 730K MPS	Multiple SCP-Worker pods restart when the cache pods get into a restart state when the traffic is running at 730K MPS.	Forceful or ungraceful shutdown of all cache pods at the same time while high rate limit traffic is in progress, leading to SCP-Worker pod restart. **Workaround**: Cache pods are deployed on different worker nodes, therefore avoid all cache pods to go down at the same time.	3	25.1.100
37428245	scp does not show profile details for NF-TYPE= SCP under edit profile option	While editing NF Profiles under NF Services of SCP, it shows profile details as empty.	Edit NF-Profiles under NF-Services of SCP shows profile details as empty on the CNC Console when service block does not exist. **Workaround**: There is no workaround available.	3	25.1.100

Table 4-40 (Cont.) SCP 25.1.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37640288	SCP 24.2.2 - Possibility to create subscriptions using the fqdn for TLS purpose	The implementation of SCP with NRF in TLS is not functioning. As the subscriptions are created with the IP address, SCP fails to receive notifications due to the the NRF verification process that requires FQDN.	It requires a functionality to enable the IP address for connection, but SCP still uses FQDN in the callback URI to NRF. **Workaround**: There is no workaround available.	3	24.2.2
37565543	SCP:24.2.1 Alert triggered SCPEgressTrafficRoutedWithoutRateLimitTreatment without ERL enabled	The SCPEgressTrafficRoutedWithoutRateLimitTreatment alert is raised for service name "nnrf-nfm" and NFtype NRF, even without enabling Global Egress Rate Limiting or Egress Rate Limiting for the local site.	Alert is raised for unknown FQDNs. **Workaround**: Either configure rate limit rule for unknown FQDN or register the profile to make FQDN known.	3	24.2.1
37651078	SCP creates more than 1 subscription for an nfType upon changing TSI from Local to NRF	When SCP is configured with TSI, SCP sends more than 22 subscriptions to NRF.	SCP intermittently sends duplicate subscription requests when changing the TSI. **Workaround**: Duplicate subscriptions might be created, which will not be refreshed by SCP, therefore the subscriptions are deleted after the validity time expires.	3	24.3.0

Table 4-40 (Cont.) SCP 25.1.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36245570	SCP returning undefined error when we edit NF Rule Profile Configuration	While editing the NF Rule Profile configuration after modifying the NRF SRV configuration, SCP returns 404 error that does not get cleared unless the page is refreshed.	Edit the NF Rule profile configuration after modifying NRF SRV configuration, and it displays 404 error on the CNC Console. **Workaround**: Issue is resolved with page refresh.	3	23.4.0
36173358	SCP Unable to forward notification requests when request is received with FQDN at profile level and DNS is not configured to resolve the FQDN.	SCP is unable to forward SMF notifications received from PCF to SMF.	FQDN for notification request is not resolved from profile level IP address.	3	23.3.0
37511517	During SCP overload scenario(200%), Request and Reponse processing time for SCP exceeded 2 seconds	While performing an upgrade and rollback, SCP's request and response processing time is exceeding 10 seconds.	SCP may increase request and response processing time in extreme load conditions. **Workaround**: Processing time decreases when the load is reduced to normal levels.	3	24.2.3

4.3.9 SEPP Known Bugs

Release 25.1.102

There are no known bugs in this release.

Release 25.1.101

There are no known bugs in this release.

Release 25.1.100

Table 4-41 SEPP 25.1.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
37738503	SEPP returns 500 error, instead of configured one, when timestamp format does not meet the requirement	When the Cat-3 feature is enabled, the authentication-status response from UDR has a timestamp in the following format: "timeStamp": "2018-01-02T08:17:14Z" and does not include milliseconds. SEPP returns athe 500 Internal Server Error instead of 406.	The 500 Internal Server Error is observed instead of the configured error, which is misleading. **Workaround:** There is no workaround available.	3	25.1.100
37744123	Intermittent NPE reported in pn32f logs at 10 TPS when Cat3 time check is enabled	A Null Pointer Exception is reported intermittently in the pn32f logs when the Cat-3 Time Check for Roaming Subscribers feature is enabled and traffic is at 10 TPS.	A null pointer exception is observed intermittently in the pn32f pod logs when the Cat-3 Time Check for Roaming Subscribers feature is enabled. **Workaround:** There is no workaround available.	3	25.1.100

Table 4-41 (Cont.) SEPP 25.1.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
37669351	Need assistance to test Health Check Feature	The SCP Health Check request rate increases when the peer monitoring configuration is modified. This increase in the health check request rate can be tracked using: `rate(oc_egressgateway_peer_health_ping_request_total{namespace=~"namespace"}[2m])`	The health check message frequency does not match the configured values, and the number of health check messages is higher than expected.' **Workaround:** Perform one of the following workarounds: - Restart the N32 EGW pod: After restarting the pod, the EGW thread pools are reinitialized, and the health API rate will align with the configuration. - Increase the peer monitoring configuration frequency: To minimize the health API queries per second, you can increase the frequenc	3	24.3.1

Table 4-41 (Cont.) SEPP 25.1.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
			y. This configuration change can be made without requiring a restart.		
37755073	Too many TCP connections from SEPP to UDM	A very high number of TCP connections is observed towards the outbound NF UDM from the SEPP PLMN Egress Gateway. The PLMN Egress Gateway is opening a new TCP connection with almost every new request when the Jetty idle timeout is set to 0.	• The maximum connections per IP are not being honored, resulting in a higher number of connections than configured. • This scenario leads to an increased number of inactive connections. **Workaround:** There is no workaround available.	3	24.3.1
37757758	changing RSS priorites after removing primary SEPP	After removing the Primary SEPP from the Remote SEPP Set, the SEPP reversed the priorities of the secondary and tertiary SEPPs in the Remote SEPP Set.	There is no impact on live traffic, but impact on ATS test cases. **Workaround:** There is no workaround available.	3	24.3.1

Table 4-41 (Cont.) SEPP 25.1.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
37680589	SEPP TUH header path for deregistration notification does not work	The SEPP is unable to run Topology Unhiding (TUH) for the NFInstanceId in the deregistration notification header path from UDM to AMF and is not running TUH on the header path for the deregistration-notification callback.	Deregistration notifications from UDM to AMF fail for all subscribers if the Topology Hiding feature is turned ON. **Workaround:** There is no workaround available.	3	24.2.1
37671533	Some call fail and some error observed with code 500,504 and 406 during 20K MPS performance run with feature enable at sepp_25.1.100-rc3	During high-performance testing, some calls failed, and errors with codes 500, 504, and 406 were observed during a 20K MPS performance run with the features enabled at SEPP 25.1.100.	Some of the intermittent messages result in an error response. **Workaround:** There is no workaround available.	3	25.1.100

Table 4-41 (Cont.) SEPP 25.1.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
37587256	Request guidance on how to accommodate for 2 and 3 digit MNCs for CAT2 screening in SEPP	In the Security Counter Measure Cat-2 feature, rules are defined to filter specific requests. When configuring these rules, the length of the MNC must be defined as either 2 or 3. Since there is only one rule for both directions, if the MNC length differs between the two countries, the filtering rule will not work in one direction.	If the MNC length differs between the two countries, the filtering rule in the Cat-2 feature will not work in one direction. **Workaround:** There is no workaround available.	3	24.3.0

Table 4-41 (Cont.) SEPP 25.1.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
37514476	Message schema validation failing in SEPP	When the Cat-0 feature is enabled, and the visiting AMF sends a `/nudm-sdm/v2/{supi}` request to the home UDM through SEPP, SEPP blocks the request and throws the 406 error. The SEPP message validation schema expects dataset names to be in square brackets. The same issue occurs with `/nnrf-disc`. However, as per 3GPP TS 29.501, dataset names are an array of "simple types", and the formatting does not include square brackets or double quotes.	The `/nudm-sdm/v2/{supi}` message fails when the Cat-0 feature is enabled. **Workaround:** In the Cat- 0 Message Schema configuration for `/nudm-sdm/v2/{supi}` API, remove the entry for the dataset names schema. This step skips the validation for the dataset-names parameter.	3	24.2.0

Table 4-41 (Cont.) SEPP 25.1.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release

37499126	Ratelimit failing when header contains srcinfo	The header validation fails when the source information is included. If only the origin PLMN is included, the validation is done correctly.
		Header failing:
		`3gpp-sbi-originating-network-id: 310-014; src: SEPPsepp001.sepp.5gc.mnc014.mcc310.3gppnetwork.org`
		Header working fine:
		`3gpp-sbi-originating-network-id: 310-014`
			When the Rate Limiting feature is turned on and the header contains the `src` parameter, rate limiting will not be applied to the message.
			Workaround:
			None
				3	23.1.1

Table 4-41 (Cont.) SEPP 25.1.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
35898970	DNS SRV Support- The time taken for cache update is not same TTL value defined in SRV record.	The time taken to update the cache does not align with the TTL defined in the SRV records. Sometimes, the cache updates before the TTL expires, while at other times, it updates later than the TTL. Expectation: The cache should update according to the TTL. For example, if the TTL is set to 60 seconds, the cache should update exactly after every 60 seconds once the TTL expires.	If the priority or weight is changed, it may take longer than the TTL for the cache to update and reflect the changes in the environment. **Workaround**: After changing the configuration, restart the n32-egress-gateway and alternate-route-svc.	3	23.4.0

Table 4-41 (Cont.) SEPP 25.1.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
36614527	[SEPP-APIGW] Overload Control discard policies not working with REST API and CNCC	The default values for Overload Control discard policies can not be edited or changed. An error message, "ocpolicymapping does not contain this policy name," is thrown when saving the configuration. The same behavior is observed with the REST API.	The user cannot edit overload discard policies through the CNC Console. **Workaround**: Helm configuration is used to configure overload discard policies.	3	24.2.0
36605744	Generic error is thrown when wrong configuration is saved via GW REST APIs	A generic error ("Could not validate JSON") is thrown when an incorrect configuration is saved via the Gateway REST APIs or CNC Console screen. The error message should be more specific, indicating which mandatory parameter is missing.	A generic error makes it difficult for the user to troubleshoot the issue. **Workaround**: There is no workaround available.	3	24.2.0

Table 4-41 (Cont.) SEPP 25.1.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
36672487	No error thrown while enabling Discard Policy Mapping to true when corresponding discard policy is deleted	No error is thrown when enabling Discard Policy Mapping to true while the corresponding discard policy has been deleted. **Steps to reproduce:** 1. Delete the discard policy "Policy2" from the Overload discard policies of n32-igw. 2. Enable the discard policy in Discard Policy Mapping to true, with the policy name set to "Policy2." The configuration is saved successfully, but an error should be thrown, as the Discard Policy "Policy2" has been deleted.	If the user enables Discard Policy Mapping to true and the discard policy does not exist, no error will be visible. **Workaround**: Helm configuration can be used to configure overload discard policies.	3	24.2.0

Table 4-41 (Cont.) SEPP 25.1.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
36263009	PerfInfo calculating ambiguous values for CPU usage when multiple services mapped to single pod	In the cgroup.json file, multiple services are mapped to a single endpoint, making the calculation of CPU usage ambiguous. This impacts the overall load calculation.	Overall load calculation is not correct. **Workaround**: There is no workaround available.	3	23.4.1

Table 4-41 (Cont.) SEPP 25.1.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
35919133	DNS SRV Support-Custom values key "dnsSrvEnabled" does not function as decsribed	**Problem Statement:** The description for the custom values key `dnsSrvEnabled` mentions its use as a flag to control whether DNS-SRV queries are sent to coreDNS. **Interpretation:** If the flag is true, requests should be sent to coreDNS. If the flag is false, requests must not be sent to coreDNS. **Issue:** Even when the flag is set to false and the setup is upgraded, the curl request still reaches coreDNS. **Scenario:** When the flag is set to false and peerconfig is created for the Virtual FQDN, the expectation is that executing the curl request should not resolve the Virtual FQDN, as the flag is false. Therefore, the request should not	In the case of a virtual FQDN, the query always goes to coreDNS. **Workaround**: Do not configure records in coreDNS.	3	23.4.0

Table 4-41 (Cont.) SEPP 25.1.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
		reach coreDNS.			
37670498	ERROR LOG in SEPP config manager pod and Performance pod	Continuous Error logs in SEPP are observed in the config-manager pod and performance pod as follows: SEPP Config Manager pod logs: The Config Manager pod is continuously generating Error logs for connector/J, indicating the need to use autoreconnect =true as the client timeout is being hit. SEPP performance pod logs: We have observed that the performance pod is incorrectly making a curl request to the n32-igw service on port 80, which is not exposed by the service.	Error messages are observed in both the config-mgr-svc and performance pods. **Workaround:** There is no workaround available.	4	24.2.1

Table 4-41 (Cont.) SEPP 25.1.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
37720757	different validation for mcc on CNCC and REST for MCC Exception list	Different validations for MCC on CNC Console and REST for the MCC Exception list are performed. The validation through CNC Console is correct, but the REST API, when triggered directly, accepts MCC values starting with 0.	No impact on traffic. The user can configure an incorrect MCC value in the 'MCC Exception list' through REST API. **Workaround:** Use only the CNC Console for configuration.	4	25.1.100
37640294	Prometheus uses different ports for different micorservices	Different SEPP services are using different Prometheus ports. The requirement is to make the ports uniform across all services.	The user has to create a different service monitor to cover all the metrics from OCSEPP. **Workaround:** There is no workaround available.	4	23.2.0

4.3.10 UDR Known Bugs

Release 25.1.100

Table 4-42 UDR 25.1.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37501534	SLF_Controlled_shutdown not working after helm upgrade	SLF Controlled Shutdown feature is not working after Helm upgrade.	Controlled Shutdown feature is impacted. **Workaround**: Use UDR as the nfType.	3	24.2.0

Table 4-42 (Cont.) UDR 25.1.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37777519	SLF 25.1.100 - Not able to change the loglevel for nrfClientManagement service	NrfClientManagement pod and loglevel is not getting changed in the NrfClient pod using CNC Console.	There is no impact as the operator can use REST API configuration to perform the changes. **Workaround**: Use REST API configuration to change the log level.	3	25.1.100

4.3.11 Common Services Known Bugs

4.3.11.1 ATS Known Bugs

Release 25.1.100

There are no known bugs in this release.

4.3.11.2 ASM Configuration Known Bugs

Release 25.1.100

There are no known bugs in this release.

4.3.11.3 Alternate Route Service Known Bugs

Release 25.1.100

There are no known bugs in this release.

4.3.11.4 Egress Gateway Known Bugs

Table 4-43 Egress Gateway 25.1.100 Known Bugs

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

Table 4-43 (Cont.) Egress Gateway 25.1.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37355062	occnp_oc_egressgateway_peer_health_status reports incorrect peer health from one pod	The `occnp_oc_egressgateway_peer_health_status` metric was getting pegged correctly on the Egress Gateway leader pod but was not getting updated on non-leader Egress Gateway pods, causing inconsistent status between a leader and a non-leader pod for the same peer.	When the metric was fetched from the non-leader pod, it was showing an incorrect status compared to the leader pod. **Workaround**: There is no workaround available.	3	23.4.3
37501092	Egress Gateway not retrying to sameNRF or Next NRF when "errorCodes: -1" for errorSetId: 5XX on retryErrorCodeSeriesForNex/SametNrf OauthClient configuration	Egress Gateway does not treat -1 as all errors codes correctly for 5XX errors as it does for 4XX errors. So, when you use -1 to cover all 5XX errors, it does not work as expected.	Any rule that depends on -1 to catch all 5XX errors may not work. **Workaround**: There is no workaround available.	3	24.2.5
37451580	Metric not getting pegged after health ping request is sent towards a peer	The required number of parameters to peg `oc_egressgateway_peer_health_ping_request_total` and `oc_egressgateway_peer_health_ping_response_total` metrics were inconsistent when vfqdn was present and vfqdn was absent.	The metric was showing inconsistent behavior while pegging. **Workaround**: There is no workaround available.	4	24.2.9

4.3.11.5 Ingress Gateway Known Bugs

Table 4-44 Ingress Gateway 25.1.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36677373	NRF- Missing mandatory "iat claim" parameter validation is not happening in CCA header for feature - CCA Header Validation	As per the feature description, "iat" is a mandatory parameter in JWT claims. When CCA header request is sent without "iat" claim and "maxTokenAge": 0 is set in /nrf/nf-common-component/v1/igw/ccaheader. The missing mandatory parameter is not validated, and the CCA header request gets accepted by NRF.	Mandatory validation to be performed on parameter would be missed at Gateway Services and request would be processed. **Workaround**: There is no workaround available.	3	23.2.0
36464641	When feature Ingress Gateway POD Protection disabled at run time alerts are not getting cleared and metrics are getting pegged in NRF 23.4.0	When the Ingress Gateway Pod Protection feature is disabled at run time, alerts are not getting cleared and metrics are getting pegged in NRF 23.4.0.	Alerts are not getting cleared and metrics would be pegged even when feature is disabled during run time. **Workaround**: There is no workaround available.	3	23.4.0

Table 4-44 (Cont.) Ingress Gateway 25.1.100 Known Bugs

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

Table 4-44 (Cont.) Ingress Gateway 25.1.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37483564	NPE observed in IGW during traffic run	NPE is emitted by the PreGateway filter when trying to peg the response_processing_latency metric. The metric value is calculated when the response was received by the PostGateway filter and the time it took to reach the PreGateway filters. The PostGateway filter is supposed to add the ResponseReceivedTime attribute to the response. The PreGateway filter makes an assumption that ResponseReceivedTime is always present in the response. In case of discard due to overload control, the PostGateway filter is never invoked and ResponseReceivedTime is never added. The code to peg tries to get a ResponseReceivedTime attribute from the exchange, which is missing. This NPE is observed by Spring and pegged as http_server_requests_seconds_count.	NPE is emitted by the PreGateway filter when trying to peg the response_processing_latency metric. The exception was observed and handled by Spring Cloud Gateway. **Workaround**: There is no workaround available.	3	23.4.6

Table 4-44 (Cont.) Ingress Gateway 25.1.100 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37506720	Overload Discard Percentage for NRF Microservices	Ingress Gateway handles both Access Token and Discovery traffic using a single microservice and a shared configuration. Due to significant differences in traffic volumes, this approach leads to suboptimal overload control behavior.	This unified handling of both Access Token and Discovery traffic causes performance degradation, especially under high Discovery load, potentially leading to unnecessary throttling or delayed responses for Access Token requests. **Workaround**: Perform local discard to remove excess requests locally without involving coherence or global coordination mechanisms.	2	24.2.11
35913189	Missing validation of the failureReqCountErrorCodeSeriesId mandatory parameter in the Ingress Gateway's Routes Configuration	As per NSSF_REST_Specification_Guide, Section 5.2.1.5, failureReqCountErrorCodeSeriesId is a mandatory parameter for Routes Configuration in Ingress Gateway. The request is rejected by Ingress Gateway when the failureReqCountErrorCodeSeriesId parameter is not present in the JSON payload.	Requests will be processed by considering the mandatory configuration from the existing deployment configuration when it is not configured through REST APIs. **Workaround**: There is no workaround available.	4	23.3.0

4.3.11.6 Common Configuration Service Known Bugs

Release 25.1.100

There are no known bugs in this release.

4.3.11.7 Helm Test Known Bugs

Release 25.1.100

There are no known bugs in this release.

4.3.11.8 Mediation Known Bugs

Release 23.4.0

There are no known bugs in this release.

4.3.11.9 NRF-Client Known Bugs

Release 25.1.1xx

There are no known bugs in this release.

4.3.11.10 App-Info Known Bugs

Release 25.1.100

There are no known bugs in this release.

4.3.11.11 Perf-Info Known Bugs

Release 25.1.100

There are no known bugs in this release.

4.3.11.12 Debug Tool Known Bugs

Release 25.1.100

There are no known bugs in this release.