Oracle® Communications

Cloud Native Core Release Notes

Release 3.25.2.200.0
G50864-03
March 2026

Oracle Communications Cloud Native Core Release Notes, Release 3.25.2.200.0

G50864-03

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 Core cnDBTier 2
2.4 Cloud Native Configuration Console (CNC Console) 5
2.5 Cloud Native Environment (CNE) 6
2.6 Network Slice Selection Function (NSSF) 8
2.7 Oracle Communications Cloud Native Core, Certificate Management (OCCM) 10
2.8 Operations Services Overlay (OSO) 11

3 Media and Documentation

3.1 Media Pack 1
3.2 Documentation Artifacts with MOS Patch Numbers 4
3.3 Compatibility Matrix 4
3.4 3GPP Compatibility Matrix 6
3.5 Common Microservices Load Lineup 7
3.6 Generic Open Source Software Compatibility on Any Platform 8
3.7 Redhat Openshift Compliance Matrix 16
3.8 Security Certification Declaration 16
3.8.1 BSF Security Certification Declaration 17
3.8.2 CNC Console Security Certification Declaration 17
3.8.3 cnDBTier Security Certification Declaration 18
3.8.4 OCCM Security Certification Declaration 18
3.8.5 NSSF Security Certification Declaration 19

4 Resolved and Known Bugs

4.1 Severity Definitions 1
4.2 Resolved Bug List 2
4.2.1 ATS Resolved Bugs 2

4.2.2 BSF Resolved Bugs 3
4.2.3 cnDBTier Resolved Bugs 13
4.2.4 CNC Console Resolved Bugs 34
4.2.5 CNE Resolved Bugs 35
4.2.6 NSSF Resolved Bugs 36
4.2.7 OSO Resolved Bugs 42
4.2.8 OCCM Resolved Bugs 43
4.2.9 Common Services Resolved Bugs 43
4.2.9.1 Egress Gateway Resolved Bugs 43
4.2.9.2 Ingress Gateway Resolved Bugs 46
4.2.9.3 Alternate Route Service Resolved Bugs 49
4.2.9.4 Common Configuration Service Resolved Bugs 51
4.2.9.5 NRF-Client Resolved Bugs 51
4.3 Known Bug List 52
4.3.1 ATS Known Bugs 52
4.3.2 BSF Known Bugs 52
4.3.3 CNC Console Known Bugs 53
4.3.4 cnDBTier Known Bugs 54
4.3.5 CNE Known Bugs 56
4.3.6 NSSF Known Bugs 57
4.3.7 OCCM Known Bugs 69
4.3.8 OSO Known Bugs 70
4.3.9 Common Services Known Bugs 70
4.3.9.1 Alternate Route Service Known Bugs 70
4.3.9.2 Egress Gateway Known Bugs 71
4.3.9.3 Ingress Gateway Known Bugs 80
4.3.9.4 Common Configuration Service Known Bugs 84

Preface

- Documentation Accessibility
- Diversity and Inclusion
- Conventions

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which user supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that user enter.

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 3.25.2.200.0 - G50864-03, March 2026

Added the following known bugs in the Egress Gateway Known Bugs section:

- 39088228
- 39123626
- 39083890
- 39049678

Release 3.25.2.200.0 - G50864-02, March 2026

- Updated the description of **Support for SBI-Message Priority** and **BSF support for the Even CPUs profile** features in the Binding Support Function (BSF) section.
- Updated CNE upgrade path in the Media Pack section.

Release 3.25.2.200.0 - G50864-01, March 2026

General Updates:

- Updated the open source software compatibility information in the Generic Open Source Software Compatibility on Any Platform section.
- Updated the MOS patch details in the Documentation Artifacts with MOS Patch Numbers section.
- Updated Redhat Openshift compliance matrix in the Redhat Openshift Compliance Matrix section.

ATS 25.2.202 Release

Updated the following sections with the details of ATS release 25.2.202:

- Automated Testing Suite (ATS) Framework
- Media Pack

BSF 25.2.200 Release

Updated the following sections with the details of BSF release 25.2.200:

- Binding Support Function (BSF)
- Media Pack
- Compatibility Matrix
- BSF Security Certification Declaration
- BSF Resolved Bugs
- BSF Known Bugs

cnDBTier 25.2.201 Release

Updated the following sections with the details of cnDBTier release 25.2.201:

- Cloud Native Core cnDBTier
- Media Pack

- Compatibility Matrix
- cnDBTier Security Certification Declaration
- cnDBTier Resolved Bugs
- cnDBTier Known Bugs

Console 25.2.200 Release

Updated the following sections with the details of Console release 25.2.200:

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

CNE 25.2.200 Release

Updated the following sections with the details of CNE release 25.2.200:

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

NSSF 25.2.200 Release

Updated the following sections with the details of NSSF release 25.2.200:

- 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 25.2.200 Release

Updated the following sections with the details of OCCM release 25.2.200:

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

- OCCM Security Certification Declaration

OSO 25.2.200 Release

Updated the following sections with the details of OSO release 25.2.200:

- Operations Services Overlay (OSO)
- Media Pack

Common Services Resolved Bugs

- Alternate Route Service Resolved Bugs
- Common Configuration Service Resolved Bugs
- Egress Gateway Resolved Bugs
- Ingress Gateway 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 3.25.2.2xx.0.

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

2.1 Automated Testing Suite (ATS) Framework

Release 25.2.202

Oracle Communications Cloud Native Core, Automated Testing Suite (ATS) Framework 25.2.202 includes the following enhancements:

- **Token-based Authentication for Prometheus**:
  This enhancement enables ATS to communicate with Prometheus which requires service account token based authentication and with TLS. Service account should be given necessary role-based access control (RBAC) permissions for authorization.

  For more information, see the "ATS Feature Activation and Deactivation" section in *Oracle Communications Cloud Native Core Automated Testing Suite Guide*.
- **Support for Dual Stack**:
  The dual stack mechanism establishes connections with REST APIs and ATS GUI in a Kubernetes cluster using IPv4 or IPv6 or both simultaneously.

  For more information, see the "ATS API" section in *Oracle Communications Cloud Native Core Automated Testing Suite Guide*.

2.2 Binding Support Function (BSF)

Release 25.2.200

Oracle Communications Cloud Native Core, Binding Support Function (BSF) 25.2.200 includes the following enhancements:

- **Support for SBI Message Priority**:
  BSF supports adding `3gpp-Sbi-Message-Priority` header to all the requests that it sends out and also in all the responses that it receives from other NFs. Using `3gpp-Sbi-Message-Priority` header in requests such as REGISTER, DEREGISTER, or DISCOVERY, BSF and the associated producers and consumers such as SCP, NRF, PCF, AF, and NEF can distinguish between high-priority and low-priority Service Based Interface (SBI) messages.

  Configuration Status: Disabled by default.

  For more information, see the "Support for SBI Message Priority Header" section in *Oracle Communications Cloud Native Core, Binding Support Function User Guide*.
- **Support for cnDBTier Georeplication Status Across All Sites API in CNC Console**:

This enhancement allows Georeplication Status Across All Sites APIs to be integrated into the CNC Console, and users can view the georeplication status for the site to the mated sites along with the replication group status on the CNC Console.

For more information, see "cnDBTier APIs" in *Oracle Communications Cloud Native Core, Network Repository Function User Guide*.

- **Support for Even CPUs Profile:**
  The Kubernetes CPU Manager is configured with the static or shared CPU policy to reduce deployment failures, mitigate noisy-neighbor effects, and ensure consistent CPU availability for critical network function (NF) workloads in the 5G Core environment. As part of this feature, resource profiling got updated to allocate an even number of CPUs to all BSF services and the Istio sidecar, optimizing guaranteed CPU resources per service.

  Configuration Status: Enabled by default.

  For details on the resource requirements for installing BSF, see "Resource Requirements" section in *Oracle Communications Cloud Native Core, Binding Support Function Installation, Upgrade, and Fault Recovery Guide*.

- **Application Framework Change**: Spring Boot has been replaced with Micronaut as the framework for microservices (except Alternate Route Service, Ingress gateway or Egress gateway micro services).
  For more information, see the "Application Framework Change" 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-1345	Support for SBI Message Priority
Oracle Communications Cloud Native Core, Binding Support Function - 25K Active Subscribers Perpetual	CCNC-11758	Support for cnDBTier Georeplication Status Across All Sites APIs in CNC Console
Oracle Communications Cloud Native Core, Binding Support Function - 25K Active Subscribers Perpetual	CCNC-11677	Support for Even CPUs Profile

2.3 Cloud Native Core cnDBTier

Release 25.2.201

Oracle Communications Cloud Native Core, cnDBTier (cnDBTier) 25.2.201 includes the following enhancements:

- **Support for Parallel Restart of cnDBTier Pods**

  This release introduces the ability to create, delete, and update pods within a StatefulSet concurrently rather than sequentially. This significantly reduces maintenance windows and rollout times while ensuring stability and data integrity. Users can utilize this functionality by running the `dbtupgrade_parallel_restart` script.

  Configuration Status: Always enabled (no additional configuration required)

For more information, see the "Performing a Parallel Restart of cnDBTier Pods" section in *Oracle Communications Cloud Native Core, cnDBTier User Guide*.

- **Enhanced Georeplication Monitoring in CNC Console**

  A new screen in the CNC Console provides a centralized interface to monitor and verify georeplication status across all configured sites.

  To support this UI enhancement, the following REST APIs are now available:

  - http://base-uri/ocdbtier/faultrecovery/start
  - http://base-uri/ocdbtier/v1/backup/status
  - http://base-uri/ocdbtier/replication/status/realtime
  - http://base-uri/ocdbtier/replication/status/realtime/{siteName,remoteSiteName}

  Configuration Status: Always enabled (no additional configuration required)

  For more information, see the following sections:

  - For the REST APIs, see the "cnDBTier APIs for CNC Console" section in *Oracle Communications Cloud Native Core, cnDBTier User Guide.*
  - For the enhanced CNC Console screen, see the "Monitoring Georeplication Recovery Status Using CNC Console" section in *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide.*

- **Georeplication Recovery (GRR) Performance Improvement**

  To support for both manual and automated recovery, improved site selection, and better monitoring for seamless cnDBTier replication restoration, the following configuration parameters have been updated:

  Added the following global configuration parameters to support backup restoration process in Georeplication Recovery in the Global Parameters section:

  - `/global/additionalndbconfigurations/ndb/MaxFKBuildBatchSize` with default value `512`
  - `/global/additionalndbconfigurations/ndb/MaxUIBuildBatchSize` with default value `512`

  Updated the default values for the following parameters:

  - `global/ndb/restoreparallelism` from `128` to `1024`
  - `ndb/resources/requests/memory` from `16Gi` to `18Gi`
  - `api/resources/limits/CPU` from `8` to `4`
  - `api/resources/requests/CPU` from `8` to `4`
  - `db-replication-svc/resources/limits/CPU` from `1` to `1.1`
  - `db-replication-svc/resources/requests/CPU` from `0.6` to `1`
  - `db-backup-manager-svc/resources/limits/cpu` from `1` to `1.1`
  - `db-backup-manager-svc/resources/requests/cpu` from `1` to `1.1`

  Configuration Status: Always enabled (no additional configuration required)

  For more information, see the "Customizing cnDBTier" section in *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*.

- **Automated Horizontal Scaling of NDB Pods**

The procedure for scaling `ndbappmysqld` pods has been updated to utilize the `dbtscale_ndbmtd_pods` script. This tool automates the expansion of cnDBTier clusters, allowing for seamless scaling of NDB data pods to meet increased capacity demands.

Configuration Status: Always enabled (no additional configuration required)

For more information, see the "Horizontal Scaling of ndbmtd pods using dbtscale_ndbmtd_pods" section in *Oracle Communications Cloud Native Core, cnDBTier User Guide*.

- **Addition of cnDBTier Georedundant Site**
  The procedure to add cnDBTier georedundant mate site has been updated to include the procedure to scale db replication service deployments and ndbmysqld pods.

  Configuration Status: Always enabled (no additional configuration required)

  For more information, see the "Scaling of db replication service deployments and ndbmysqld pod" section in *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*.

- **Schema and Data Consistency Georeplication Audit**

  In a cnDBTier deployment, georeplicated database sites can be monitored using the dbtaudit script. This command-line utility allows administrators to audit site status, review replication health, and ensure overall compliance across distributed database clusters.

  Configuration Status: Always enabled (no additional configuration required)

  For more information, see the "Auditing georeplicated database sites using dbtaudit script" section in *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*.

- **Aspen Service Mesh (ASM) for External Communication**:
  This feature enables secure external communication through ASM (Application Service Mesh) by selectively applying Istio sidecar injection only to pods where external communication is involved. By selectively enforcing ASM policies, cnDBTier ensures the security and compliance of its external interfaces, while preserving high performance and simplifying manageability within the cnDBTier ecosystem.

  Configuration Status: Disabled by default.

  For more information, see the "Aspen Service Mesh (ASM) for External Communication" section in *Oracle Communications Cloud Native Core, cnDBTier 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 2-2 License names for feature mapping

License Name	CCNC Number	Feature Name
Oracle Communications Cloud Native Core, Cloud Native Environment - per 25K Subscribers Perpetual	CCNC-11640	Parallel Restart of cnDBTier Pods
Oracle Communications Cloud Native Core, Cloud Native Environment - per 25K Subscribers Perpetual	CCNC-11227	Georeplication Performance Improvement
Oracle Communications Cloud Native Core, Cloud Native Environment - per 25K Subscribers Perpetual	CCNC-10389	Automated Horizontal Scaling of NDB Pods

2.4 Cloud Native Configuration Console (CNC Console)

Release 25.2.200

Oracle Communications Cloud Native Configuration Console (CNC Console) 25.2.200 includes the following enhancements:

- **CNC Console IAM Backend Upliftment**:

  CNC Console has performed an IAM backend upliftment to resolve security issues, theme updates, and handle database schema changes. As a part of this upliftment, the core procedures for adding or updating passwords, creating and viewing users, configuring SAML IDP, generating access tokens, and managing user federation remain functionally unchanged. However, the UI screens have been refreshed to align with the latest interface and design standards.

  Configuration Status: Enabled by default.

  For more information on this enhancement, see *Oracle Communications Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide* and *Oracle Communications Cloud Native Configuration Console User Guide.*

- **Application Framework Change:**Spring Boot has been replaced with Micronaut as the framework for microservices.

  Configuration Status: Always enabled (no additional configuration required).

- **Support for Additional cnDBTier APIs:** CNC Console now supports additional cnDBTier APIs for replication status across all cnDBTier sites. This enhancement is NF dependent and must be enabled in their respective NF configurations.

  Configuration Status: Enabled by default.

  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 Disabling mTLS/TLS for cnDBTier Internal Pod Communication:** CNC Console supports configuring ASM for external traffic only, effectively disabling mTLS for internal communication between cnDBTier pods. This enhancement provides more granular control over sidecar injection, allowing you to select from three modes: None, All, and External. This replaces the previous binary configuration. CNC Console now supports integration with cnDBTier configured in external mode.

  Configuration Status: Disabled by default.

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, Cloud Native Environment - per 25K Subscribers Perpetual	CCNC-10855	CNC Console IAM Backend Upliftment
Oracle Communications Cloud Native Core, Cloud Native Environment - per 25K Subscribers Perpetual	CCNC-10849	Support for Migration from Springboot to Micronaut

Table 2-3 (Cont.) License names for feature mapping

License Name	CCNC Number	Feature Name
Oracle Communications Cloud Native Core, Cloud Native Environment - per 25K Subscribers Perpetual	CNCC-11861	Support for Additional cnDBTier APIs
Oracle Communications Cloud Native Core, Cloud Native Environment - per 25K Subscribers Perpetual	CCNC-11968	Support for Disabling mTLS/TLS for cnDBTier Internal Pod Communication

2.5 Cloud Native Environment (CNE)

Release 25.2.200

Oracle Communications Cloud Native Core, Cloud Native Environment (CNE) 25.2.200 includes the following enhancements:

- **CNE API Server public endpoint**:

  This feature provides an option to expose the Kubernetes API server as a public endpoint. The public endpoint is secured using mutual TLS (mTLS) authentication and provides admin-level access to the cluster. This capability supports use cases such as enabling GitOps workflows, while maintaining robust security controls.

  Configuration Status: Disabled by default.

  For more information, see the "Enabling Public Endpoint for CNE (Kubernetes) API Server" section in *Oracle Communications Cloud Native Core, Cloud Native Environment User Guide.*

- **CNLB Support for Egress and Ingress Bypass (OpenStack Only)**:

  This feature allows applications to use network attachments that route traffic directly through the native Multus interface, effectively bypassing CNLB.

  > **Note**
  >
  > This feature requires a fresh CNE installation and is available exclusively on the OpenStack platform.

  Configuration Status: Always enabled (no additional configuration required)

  For more information, see the "CNLB Bypass Configuration" section in *Oracle Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide.*

- **CNLB Connection Synchronization**:
  Connection synchronization is now supported between active and standby CNLB application pods. This enhancement preserves live CNLB connections during switchover events, delivering seamless user experience and preventing connection drops.

  Configuration Status: Disabled by default.

  For more information on Connection synchronization, see the following sections in *Oracle Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide*:

  - For enabling and disabling connection tracking feature, see "Managing Connection Tracking Feature" subsection in the "Configuring Cloud Native Load Balancer (CNLB)" section.
  - For configurable parameters, see "CNLB Manager Environment Variables" table in the "Configuring Cloud Native Load Balancer (CNLB)" section.

- **Dedicated Nodes for CNLB**:
  CNE now supports the creation of dedicated nodes reserved exclusively for CNLB. These nodes do not host any other workloads, except observability workloads. It is recommended to use this feature in conjunction with the Heterogeneous Nodes enhancement for optimal deployment flexibility.

  Configuration Status: Always enabled (no additional configuration required)

  For more information, see the "CNLB Deployment Strategies" section in *Oracle Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide.*

- **Support for Heterogeneous Node Types**:
  Clusters can now be created with up to three different OpenStack VM flavors (small, medium, and large). This enhancement allows for optimized resource allocation within a cluster. For CNLB workloads, using the small flavor is recommended to maximize efficiency and resource utilization.

  > **Note**
  >
  > This feature requires a fresh CNE installation and is available only on the vCNE platform in this release.

  Configuration Status: Always enabled (no additional configuration required)

  For more information, see the "CNLB Deployment Strategies" section in *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 - 3.19.1
  - Kubernetes - 1.34.2
  - containerd - 2.1.4
  - Calico - 3.30.3
  - MetalLB - 0.15.2
  - Prometheus - 3.6.0
  - OCI-Grafana - 7.5.17
  - Jaeger - 1.72.0
  - Istio - 1.18.2
  - Kyverno - 1.15.0
  - cert-manager - 1.12.4

  To get the complete list of third-party services and their versions, refer to the dependencies_25.2.200.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 2-4 License names for feature mapping

License Name	CCNC Number	Feature Name
Oracle Communications Cloud Native Core, Advanced Cloud Native Environment – 25K Active Subscribers Perpetual	CCNC-11487	Support for Heterogeneous Node Types
Oracle Communications Cloud Native Core, Advanced Cloud Native Environment – 25K Active Subscribers Perpetual	CCNC-11459	CNLB Support for Egress and Ingress Bypass (OpenStack Only)
Oracle Communications Cloud Native Core, Advanced Cloud Native Environment – 25K Active Subscribers Perpetual	CCNC-11342	cnLB optimization to increase the performance on Ingress or Egress or Mix per Service IP for OpenStack -25.2.200
Oracle Communications Cloud Native Core, Advanced Cloud Native Environment – 25K Active Subscribers Perpetual	CCNC-11172	Dedicated Nodes for CNLB
Oracle Communications Cloud Native Core, Advanced Cloud Native Environment – 25K Active Subscribers Perpetual	CCNC-10453	CNLB Connection Synchronization

2.6 Network Slice Selection Function (NSSF)

Release 25.2.200

Oracle Communications Cloud Native Core, Network Slice Selection Function (NSSF) 25.2.200 includes the following enhancements:

- **Application Framework Change:** Spring Boot has been replaced with Micronaut as the framework for microservices. With this migration, support for the latency metric `*_latency_seconds` has been deprecated.

  Configuration Status: Always enabled (no additional configuration required)

  For more information, see the “NSSF Metrics” section in *Oracle Communications Cloud Native Core, Network Slice Selection Function User Guide*.
- **NRF Client Retry and Health Check:** The NRF Client Health Check continuously assesses the health of NRF instances to ensure high availability and seamless failover, especially in georedundant environments. It includes configurable intervals, intelligent health status updates, and a retry mechanism to minimize service disruption.

  Configuration Status: Enabled by default.

For more information, see “NRF Client Retry and Health Check” section in *Oracle Communications Cloud Native Core, Network Slice Selection Function User Guide*.

- **Support for TLSv1.3 on Internal API Communication:** NSSF supports TLSv1.3 (in addition to TLSv1.2) for secure communication with the Kubernetes API server.

  Configuration Status: Disabled by default.

  For more information, see “Support for TLSv1.3 on Internal API Communication” section in *Oracle Communications Cloud Native Core, Network Slice Selection Function User Guide*.

- **Support for Dual Stack:** Using the dual stack mechanism, NSSF communicates within services or deployments in a Kubernetes cluster using IPv4 or IPv6 or both simultaneously depending on the configured deployment mode.

  Configuration Status: Always enabled (no additional configuration required)

  For more information, see “Support for Dual Stack” section in *Oracle Communications Cloud Native Core, Network Slice Selection Function User Guide*.

- **Support for Disabling mTLS/TLS for cnDBTier Internal Pod Communication:** CNC Console supports configuring ASM for external traffic only, effectively disabling mTLS for internal communication between cnDBTier pods. This enhancement provides more granular control over sidecar injection, allowing you to select from three modes: None, All, and External. This replaces the previous binary configuration. CNC Console now uses external mode to integrate with cnDBTier and you can deploy cnDBTier without ASM sidecars for internal pod communication.

  Configuration Status: Enabled by default.

  For more information, see “Configuring NSSF to Support Aspen Service Mesh” section in *Oracle Communications Cloud Native Core, Network Slice Selection Function Installation, Upgrade, and Fault Recovery Guide*.

- **Support for ASM 1.21.6:** NSSF supports Aspen Service Mesh (ASM) 1.21.6 from this release.

  For more information, see “Configuring NSSF to Support Aspen Service Mesh” section in *Oracle Communications Cloud Native Core, Network Slice Selection Function Installation, Upgrade, and Fault Recovery Guide*.

- **Support for Grafana 7.5.x:** NSSF supports Grafana version 7.5.x.

  Configuration Status: Enabled by default.

  For more information, see “Software Requirements” section in *Oracle Communications Cloud Native Core, Network Slice Selection Function 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 2-5 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-11959	Support for Disabling mTLS/TLS for cnDBTier Internal Pod Communication
Oracle Communications Cloud Native Core, Network Slice Selection Function - 25K Active Subscribers Perpetual	CCNC-11377	NSSF: Support for ASM 1.21.6

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

License Name	CCNC Number	Feature Name
Oracle Communications Cloud Native Core, Advance Networking - 25K Active Subscribers	CCNC-11118	Support for Dual Stack
Oracle Communications Cloud Native Core, Network Slice Selection Function - 25K Active Subscribers Perpetual	CCNC-10668	Support for Grafana 7.5.x
Oracle Communications Cloud Native Core, Network Slice Selection Function - 25K Active Subscribers Perpetual	CCNC-10361	NSSF: S-nssai to be configured at PLMN level
Oracle Communications Cloud Native Core, Network Slice Selection Function - 25K Active Subscribers Perpetual	CCNC-9884	Application Framework Change
Oracle Communications Cloud Native Core, Network Slice Selection Function - 25K Active Subscribers Perpetual	CCNC-9153	Support for TLSv1.3 on Internal API Communication
Oracle Communications Cloud Native Core, Network Slice Selection Function - 25K Active Subscribers Perpetual	CCNC-9234	NRF Client Retry and Health Check

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

Release 25.2.200

Oracle Communications Cloud Native Core, Certificate Management (OCCM) 25.2.200 includes the following enhancement:

- **Support for Certificate Cloning:** OCCM supports the certificate cloning functionality. It streamlines how users create new certificates by allowing them to clone or duplicate an existing certificate's configuration. This significantly reduces manual entry, minimizes errors, and ensures consistency across certificate deployments.

  Configuration Status: Enabled by default

  For more information, see *Oracle Communications Cloud Native Core, Certificate Management User Guide.*

- **Support for Deleting Certificate Configuration and Secret:** OCCM has enhanced the delete certificate functionality support deleting the certificate and Kubernetes secret simultaneously. This enables the user to delete the associated Kubernetes secret along with the certificate configuration in a single action.

  Configuration Status: Always enabled (no additional configuration required)

  For more information, see *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 2-6 License names for feature mapping

License Name	CCNC Number	Feature Name
Oracle Communications Cloud Native Core, Certificate Management - 25K Active Subscribers	CCNC-10321	Support for Certificate Cloning
Oracle Communications Cloud Native Core, Certificate Management - 25K Active Subscribers	CCNC-10622	Support for Deleting Certificate Configuration and Secret

2.8 Operations Services Overlay (OSO)

Release 25.2.200

Oracle Communications Cloud Native Core, Operations Services Overlay (OSO) 25.2.200 includes the following enhancement:

- **Alert Forwarding to Kafka**: With this feature, OSO introduces an Alert Processing Microservice (APM) that receives HTTP-based alerts from OSO(Alert manager), converts them into Kafka-compatible JSON messages, and sends the alerts to a designated Kafka partition. TLS is not supported for Kafka messages.

> **Note**
>
> In this release, TLS is not supported for Kafka messages.

Configuration Status: Disabled by default

For more details, about this feature, see the "*Alert Forwarding to Kafka*" section in *Oracle Communications Cloud Native Core, Operations Services Overlay 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, Advanced Cloud Native Environment – 25K Active Subscribers Perpetual	CCNC-10339	Alert Forwarding to Kafka

3
Media and Documentation

3.1 Media Pack

This section lists the media package for Oracle Communications Cloud Native Core 3.25.2.2xx.0. To download the media package, see 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 3.25.2.2xx.0

Description	NF Version	ATS Version	Upgrade Supported
Oracle Communications Cloud Native Core, Binding Support Function (BSF)	25.2.200	25.2.200	BSF 25.2.200 supports fresh installation and upgrade from 25.1.2xx and 25.2.1xx. 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)	25.2.200	NA	CNC Console 25.2.200 supports fresh installation and upgrade from 25.1.2xx and 25.1.1xx. For more information, see *Oracle Communications Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, cnDBTier (cnDBTier)	25.2.201	NA	cnDBTier 25.2.201 supports fresh installation and upgrade from 25.1.2xx and 25.1.1xx. For more information, see *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*.

Table 3-1 (Cont.) Media Pack Contents for Oracle Communications Cloud Native Core 3.25.2.2xx.0

Description	NF Version	ATS Version	Upgrade Supported
Oracle Communications Cloud Native Core, Cloud Native Environment (CNE)	25.2.200	NA	CNE 25.2.200 supports fresh installation and upgrade from 25.1.2xx and 25.1.1xx. For more information, see *Oracle Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide*. **Note**: In-service upgrades are not supported for OpenStack CNE deployments; however, they are supported for vCNE and Bare Metal environments.
Oracle Communications Cloud Native Core, Network Slice Selection Function (NSSF)	25.2.200	25.2.200	Upgrades are not supported in this release. NSSF 25.2.200 supports fresh installation only. For more information, see *Oracle Communications Cloud Native Core, Network Slice Selection Function Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Certificate Management (OCCM)	25.2.200	NA	OCCM 25.2.200 supports fresh installation and upgrade from 25.1.2xx and 25.1.1xx. For more information, see *Oracle Communications Cloud Native Core, Certificate Management Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Operations Services Overlay (OSO)	25.2.200	NA	OSO 25.2.200 supports fresh installation and upgrade from 25.1.2xx and 25.1.1xx. For more information, see *Oracle Communications Cloud Native Core, Operations Services Overlay Installation and Upgrade 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	26.1.2xx	26.2.1xx	26.2.2xx
24.2. x	Y	Y	**NS***	NS	NS	NS	NS	NS
24.3. x	NA	Y	Y	NS	NS	NS	NS	NS
25.1.1xx	NA	NA	Y	**NS****	NS	NS	NS	NS
25.1.2xx	NA	NA	NA	Y	Y	NS	NS	NS
25.2.1xx	NA	NA	NA	NA	Y	NS	NS	NS
25.2.2xx	NA	NA	NA	NA	NA	Y	NS	NS
26.1.2xx	NA	NA	NA	NA	NA	NA	Y	Y
26.2.1xx	NA	NA	NA	NA	NA	NA	NA	Y
26.2.2xx	NA	NA	NA	NA	NA	NA	NA	NA

Legends: NS: Not Supported, NA: Not Applicable, Y: Yes, upgrade supported

Note

- ***** Policy, CNC Console, UDR, SLF, and cnDBTier supports upgrade from **24.2.x** to **25.1.2xx** (this exception applies only to upgrade from 24.2.x to 25.1.2xx).
- ****** SCP, SEPP, UDR, SLF, CNC Console, and cnDBTier supports upgrade from **25.1.1xx** to **25.2.1xx**.

For more information about the upgrade, see *Oracle Communications Cloud Native Core Solution Upgrade Guide*.

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	26.1.2xx	26.2.2xx
24.2. x	Y	NS	NS	NS	NS	NS	NS
24.3. x	NA	Y	NS	NS	NS	NS	NS
25.1.1xx	NA	NA	Y	Y	NS	NS	NS
25.1.2xx	NA	NA	NA	Y	Y	NS	NS
25.2.1xx	NA	NA	NA	NA	Y	NS	NS
25.2.2xx	NA	NA	NA	NA	NA	Y	NS
26.1.2xx	NA	NA	NA	NA	NA	NA	Y
26.2.2xx	NA	NA	NA	NA	NA	NA	NA

Legends: NS: Not Supported, NA: Not Applicable, Y: Yes, upgrade supported

> **Note**
>
> - If enabling following features in CNE, a fresh installation is required.
>   - Heterogenous Kubernetes nodes
>   - CNLB bypass for Egress traffic
>   - Dedicated CNLB Kubernetes node.
> - For vCNE-Openstack upgrade, worker node interfaces are renamed and service disruption of application traffic is expected. It is advised to do offline upgrade after diverting application traffic away form instance that is upgraded.
> - The in-service upgrades are supported only for BareMetal and VMware platforms and not for OpenStack.

For more information about the upgrade, see *Oracle Communications Cloud Native Core Solution Upgrade Guide*.

3.2 Documentation Artifacts with MOS Patch Numbers

The following table lists the availability of various documentation artifacts such as custom templates, compliance matrix, and dimensioning sheets. It also provides the MOS patch numbers of these documentation artifacts for each network function.

Table 3-2 Documentation Artifacts with MOS Patch Numbers

Network Function	NF Version	Compliance Matrix	Custom Templates	Dimensioning Sheet	MOS Patch Number
BSF	25.2.200	Y	Y	Y	39058012
CNC Console	25.2.200	NA	NA	Y	39041024
cnDBTier	25.2.201	NA	Y	Y	39054525
CNE	25.2.200	NA	Y	NA	39074022
NSSF	25.2.200	Y	Y	Y	39041018
OCCM	25.2.200	Y	NA	Y	39041030
OSO	25.2.200	NA	NA	Y	39054524

3.3 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 3-3 Compatibility Matrix

CNC NF	NF Version	CNE	cnDBTier	OSO	ASM S/W	Kubernetes	CNC Console	OCNADD	OCCM	OCI Adaptor
BSF	25.2.200	• 25.2.2x • 25.2.1x • 25.1.2x	• 25.2.2x • 25.2.1x • 25.1.2x	• 25.2.2x • 25.2.1x • 25.1.2x	1.14.6-am4	• 1.34.x • 1.33.x • 1.32.x	25.2.2xx	NA	25.2.2xx	NA
CNC Console	25.2.200	• 25.2.2x • 25.2.1x • 25.1.2x	• 25.2.2x • 25.2.1x • 25.1.2x	• 25.2.2x • 25.2.1x • 25.1.2x	• 1.21.6 • 1.14.6 • 1.11.8	• 1.34.x • 1.33.x • 1.32.x	NA	25.2.2x	25.2.2x	25.2.2x
OCCM	25.2.200	• 25.2.2x • 25.2.1x • 25.1.2x	NA	NA	NA	• 1.34.x • 1.33.x • 1.32.x	25.2.2xx	NA	NA	
CNE	25.2.200	NA	NA	NA	NA	1.34.x	NA	NA	NA	

Table 3-3 (Cont.) Compatibility Matrix

CNC NF	NF Version	CNE	cnDBTier	OSO	ASM S/W	Kubernetes	CNC Console	OCNADD	OCCM	OCI Adaptor
OSO	25.2.200	NA	NA	NA	NA	• 1.34.x • 1.33.x • 1.32.x	NA	NA	NA	NA
cnDBTier	25.2.201	• 25.2.xx • 25.2.1xx • 25.1.2xx	NA	NA	NA	• 1.34.x • 1.33.x • 1.32.x	NA	NA	NA	
NSSF	25.2.200	• 25.2.xx • 25.2.1xx • 25.1.2xx	• 25.2.xx • 25.2.1xx • 25.1.2xx	• 25.2.2xx • 25.2.1xx • 25.1.2xx	• 1.21.6 • 1.14.6	• 1.34.x • 1.32.x • 1.31.x	25.2.2xx	NA	25.2.2xx	NA
OCI Adaptor	25.2.200	NA	NA	NA	NA	1.33.x 1.32.x 1.31.x	NA	NA	NA	NA

3.4 3GPP Compatibility Matrix

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

Table 3-4 3GPP Compatibility Matrix

CNC NF	NF Version	3GPP
BSF	25.2.2xx	• 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	25.2.2xx	NA
cnDBTier	25.2.2xx	NA
NSSF	25.2.2xx	• 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	25.2.2xx	• 3GPP TS 33.310-h30 • 3GPP TR 33.876 v.0.3.0
OSO	25.2.2xx	NA

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

3.5 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 3.25.2.2xx.0.

Table 3-5 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	25.2.200	25.2.108	25.2.204	25.2.200	25.2.202	25.2.204	25.2.203	25.2.108	25.2.108	25.2.203	NA	25.2.202	25.2.204
CNC Console	25.2.100	NA	NA	NA	NA	NA	25.2.102	NA	25.2.104	25.2.102	NA	NA	NA
OCCM	25.2.100	NA	NA	NA	NA	NA	25.2.101	NA	NA	25.2.101	NA	NA	NA
NSSF	25.2.200	25.2.108	25.2.202	25.2.200	25.2.200	25.2.202	25.2.203	25.2.108	25.2.108	25.2.203	NA	25.2.202	25.2.202

3.6 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 3-6 Generic Open Source Software Compatibility on Any Platform

Software	Tested Software Version			Software Requirement	Category	Sub-Category	Category Requirement	Usage Description
	NF 25.2.2xx	NF 25.2.1xx	NF 25.1.2xx					
Kubernetes	1.33.2	1.33.1	1.32.0	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.

Table 3-6 (Cont.) Generic Open Source Software Compatibility on Any Platform

Software	Tested Software Version			Software Requirement	Category	Sub-Category	Category Requirement	Usage Description
	NF 25.2.2xx	NF 25.2.1xx	NF 25.1.2xx					
Helm	3.19.1	3.18.0	3.17.1	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.
Podman	4.9.4	4.9.4	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	2.1.4	2.0.5	1.7.24	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.

Table 3-6 (Cont.) Generic Open Source Software Compatibility on Any Platform

Software	Tested Software Version			Software Requirement	Category	Sub-Category	Category Requirement	Usage Description
	NF 25.2.2xx	NF 25.2.1xx	NF 25.1.2xx					
Velero	1.16.2	1.13.2	1.13.2	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.
Kyverno	1.15.0	1.13.4	1.13.4	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	0.15.2	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 3-6 (Cont.) Generic Open Source Software Compatibility on Any Platform

Software	Tested Software Version			Software Requirement	Category	Sub-Category	Category Requirement	Usage Description
	NF 25.2.2xx	NF 25.2.1xx	NF 25.1.2xx					
CoreDNS	1.12.0	1.12.0	1.11.3	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.
Multus	v4.2.1-thick	v4.2.1-thick	4.1.3	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 network segregation. **Impact**: Without this capability, connecting NFs to multiple networks could be limited, impacting network performance and isolation.
Fluentd	1.17.1	1.17.1	1.17.1	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.

Table 3-6 (Cont.) Generic Open Source Software Compatibility on Any Platform

Software	Tested Software Version			Software Requirement	Category	Sub-Category	Category Requirement	Usage Description
	NF 25.2.2xx	NF 25.2.1xx	NF 25.1.2xx					
OpenSearch	2.19.1	2.19.1	2.15.0	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.
OpenSearch Dashboard	2.19.1	2.19.1	2.15.0	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	0.28.0	0.28.0	0.28.0	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.

Table 3-6 (Cont.) Generic Open Source Software Compatibility on Any Platform

Software	Tested Software Version			Software Requirement	Category	Sub-Category	Category Requirement	Usage Description
	NF 25.2.2xx	NF 25.2.1xx	NF 25.1.2xx					
prometheus-kube-state-metric	2.17.0	2.16.0	2.15.0	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.
Prometheus Operator	0.85.0	0.83.0	0.80.1	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	1.10.2	1.9.1	1.8.2	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.

Table 3-6 (Cont.) Generic Open Source Software Compatibility on Any Platform

Software	Tested Software Version			Software Requirement	Category	Sub-Category	Category Requirement	Usage Description
	NF 25.2.2xx	NF 25.2.1xx	NF 25.1.2xx					
Prometheus	3.6.0	3.4.1	3.2.0	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.
Grafana	7.5.17	7.5.17	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	3.30.3	3.29.3	3.29.1	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

Table 3-6 (Cont.) Generic Open Source Software Compatibility on Any Platform

Software	Tested Software Version			Software Requirement	Category	Sub-Category	Category Requirement	Usage Description
	NF 25.2.2xx	NF 25.2.1xx	NF 25.1.2xx					
metrics-server	0.7.2	0.7.2	0.7.2	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.
snmp-notifier	2.0.0	2.0.0	1.6.1	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	1.72.0	1.69.0	1.65.0	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.
rook	1.17.7	1.16.7	1.16.6	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 3-6 (Cont.) Generic Open Source Software Compatibility on Any Platform

Software	Tested Software Version			Software Requirement	Category	Sub-Category	Category Requirement	Usage Description
	NF 25.2.2xx	NF 25.2.1xx	NF 25.1.2xx					
cinder-csi-plugin	1.33.0	1.32.0	1.32.0	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.

3.7 Redhat Openshift Compliance Matrix

The following table lists the planned Redhat Openshift compliance matrix for each network function.

Table 3-7 Redhat Openshift Compliance Matrix

CNC NF Release	Webscale	RedHat Openshift	Kubernetes	Helm	F5 ASM	F5 SPK
cnDBTier 25.2.201	1.3.x	4.7.x	1.20.x	3.12.3	1.11.8	NA
	1.5.x	4.12.x	1.25.x	3.12.3	1.14.6	1.7.11
OSO 25.2.200	1.3.x	4.7.x	1.20.x	3.12.3	1.11.8	NA
	1.5.x	4.12.x	1.25.x	3.12.3	1.14.6	1.7.11
BSF 25.2.200	1.3.x	4.7.x	1.20.x	3.12.3	1.11.8	NA
	1.5.x	4.12.x	1.25.x	3.12.3	1.14.6	1.7.11
OCCM 25.2.200	1.3.x	4.7.x	1.20.x	3.12.3	1.11.8	NA
	1.5.x	4.12.x	1.25.x	3.12.3	1.14.6	1.7.11
CNCC 25.2.200	1.3.x	4.7.x	1.20.x	3.12.3	1.11.8	NA
	1.5.x	4.12.x	1.25.x	3.12.3	1.14.6	1.7.11
NSSF 25.2.200	1.3.x	4.7.x	1.20.x	3.12.3	1.11.8	NA
	1.5.x	4.12.x	1.25.x	3.12.3	1.14.6	1.7.11

3.8 Security Certification Declaration

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

3.8.1 BSF Security Certification Declaration

Release 25.2.200

Table 3-8 BSF Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	Feb 17, 2026	No unmitigated critical or high findings
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	Jan 13, 2026	No unmitigated critical or high findings
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	Feb 24, 2026	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	Feb 24, 2026	No findings

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

3.8.2 CNC Console Security Certification Declaration

Release 25.2.200

Table 3-9 CNC Console Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	Feb 16, 2026	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 06, 2026	No unmitigated critical or high findings
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	Feb 16, 2026	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	Feb 16, 2026	No findings

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

3.8.3 cnDBTier Security Certification Declaration

Release 25.2.201

Table 3-10 cnDBTier Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	February 26, 2026	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	February 26, 2026	No unmitigated critical or high findings
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	February 26, 2026	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	February 26, 2026	No findings

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

3.8.4 OCCM Security Certification Declaration

Release 25.2.200

Table 3-11 OCCM Security Certification Declaration

Compliance Test Description	Test Completion	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	Feb 13, 2026	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 11, 2026	No unmitigated critical or high findings
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	Feb 13, 2026	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	Feb 13, 2026	No findings

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

3.8.5 NSSF Security Certification Declaration

Release 25.2.200

Table 3-12 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 10, 2026	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 10, 2026	No unmitigated critical or high findings
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	Feb 10, 2026	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	Feb 10, 2026	No findings

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

4 Resolved and Known Bugs

This chapter lists the resolved and known bugs for Oracle Communications Cloud Native Core release 3.25.2.2xx.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 3.25.2.2xx.0.

4.2.1 ATS Resolved Bugs

Release 25.2.202

Table 4-1 ATS 25.2.202 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38720772	ATS Jenkins UI fails to log in using the default policy credentials (25.2.101)	ATS login failed with default credentials. **Doc Impact:** There is no doc impact.	2	25.2.100
37735161	ATS Framework Lacks Support for ipFamilies Configuration in Helm Charts for Dual Stack Support	ATS Helm charts did not provide a configurable option to enable dual stack (IPv4 and IPv6) support. Instead, ATS relied on the Kubernetes cluster's preferred `ipFamilies` configuration, which defaulted to either IPv4 or IPv6. **Doc Impact:** There is no doc impact.	3	25.1.100

4.2.2 BSF Resolved Bugs

Release 25.2.200

Table 4-2 BSF 25.2.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release

38618278	nrfclient_nw_conn_out_request_total metric for NfDeregistration is not pegging with configured priority value	The `nrfclient_nw_conn_out_request_total` metric for `NfDeregistration` was not pegged with the following configuration. Instead, it was pegged as UNKNOWN:
		"trafficPrioritization": {
		"messageTypes": [
		{ "priority": "1", "messageType": "AutonomousOnDemandNFRegistration" },
		{ "priority": "1", "messageType": "NfHeartBeat" },
		{ "priority": "1", "messageType": "AutonomousNfPatch" },
		{ "priority": "1", "messageType": "NfDeRegistration" },
		{ "priority": "1", "messageType": "AutonomousHealthCheck" }
		],
		"featureEnabled": true,
		"incomingPriorityHeader": "3gpp-sbi-message-priority",
		"outgoingPriorityHeader": "3gpp-sbi-message-priority",
		"nfSubscribeMessageTypes": []
		}
		Doc Impact:
		There is no doc impact.
			2	25.2.200

Table 4-2 (Cont.) BSF 25.2.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
38303397	Unable to edit Load Shedding Profiles after BSF Upgrade and Rollback	After upgrading BSF from 25.1.100 to 25.1.200, the Load Shedding Profiles (LSP), LSP-overload and LSP-congestion could not be edited through CNC Console. The Edit icon did not respond. This behavior persisted after the congestion profiles were migrated and BSF was rolled back to version 25.1.100. **Doc Impact:** There is no doc impact.	2	25.1.200
38562169	XFCC_header scenarios failed while changing config-map values for Ingress Gateway when integrating APIGW	XFCC_header scenarios failed as the Ingress Gateway config-map values were changed during the APIGW integration. The `gateway` property is replaced with `gateway.server.webflux` in `application.yaml` file and in the gateways' config-map in order to address an issue in which metadata value retrieval returned `null`, because the key was treated as case insensitive. **Doc Impact:** There is no doc impact.	2	25.2.200
38840813	PCF is in complete shutdown, when PCF Diameter Gateway pod is scaled down and BSF does not perform alternate routing to PCF	Alternate routing did not function when the PCF was in complete shutdown and the Diameter gateway pods were scaled down. Diameter alternate routing was configured to route on the following error conditions (when the PCF responded): • 3002 • 3004 • timeout BSF did not route to an alternate PCF when the TCP connection was down. **Doc Impact:** There is no doc impact.	2	25.1.200

Table 4-2 (Cont.) BSF 25.2.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
38954031	log4j2_events_total metric is not seen in Prometheus for BSF Management service after performing in-service upgrade to 25.2.200. However, they are pegging correctly within the pod	During an in-service upgrade to BSF 25.2.200 from 25.2.101, the `log4j2_events_total` metric was not visible for `bsf-management-service` in the Prometheus endpoint. However, after logging into the pod and checking the metrics locally, the actuator metrics were observed to be present and updating. **Doc Impact:** There is no doc impact.	2	25.2.200
38656599	High-cardinality metrics were observed after upgrading from 25.1.100	After upgrading BSF from 25.1.100 to 25.2.200, ocbsf_diam_response_latency_seconds_bucket and ocbsf_diam_service_overall_processing_time_seconds_bucket metrics appeared to drive elevated memory utilization on the Operations Services Overlay (OSO) prom-svr pod and triggered *remote_write* errors. An out of memory condition was observed at 16 GB. After increasing the limit to 32 GB, the pod continued to restart due to overload condition. As a temporary solution, a drop action was applied on OSO to prevent scraping these metrics. After the change, the pod appeared stable, and other metrics began to display on the Grafana dashboard. Metric dimensions needed to be adjusted, so that the metrics could be used. **Doc Impact:** There is no doc impact.	3	25.1.100

Table 4-2 (Cont.) BSF 25.2.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
38636281	3002' errors were observed after Post Upgrade MOP execution for overload control change	After upgrading from BSF 23.4.x to 25.2.200, after applying the Overload and Congestion Control configurations, 3002 errors were observed for Re-Auth-Request (RAR toward Call Session Control Function (CSCF). Of the eight Diameter Gateway pods, only one Diameter Gateway pod initiated Certificates (CERs) with an outbound direction, while the remaining seven Diameter Gateway pods did not initiate CERs and reported 3002 errors for RARs. **Doc Impact:** There is no doc impact.	3	23.4.6
38786398	SCP alerts were triggered even after disabling SCP monitoring feature	SCP alerts were triggered when the SCP Peer Health Check feature was disabled. The alerts were triggered as the ocbsf_oc_egressgateway_peer_health_status != 0 expression checked for *{{Unable to render embedded object: File (= 0}.* This is because, when the feature was disabled, the metric value was set to *{{-1}},* which still satisfied the alert condition *{{} not found.= 0}}*. As a resolution, the alert condition was set to ocbsf_oc_egressgateway_peer_health_status == 1. **Doc Impact:** Updated the details of SCP_PEER_UNAVAILABLE alert in List of Alerts section in *Oracle Communications Cloud Native Core, Binding Support Function User Guide*.	3	25.1.200

Table 4-2 (Cont.) BSF 25.2.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
38854828	DateTimeParseException errors were observed in BSF Management service pod logs	The DateTimeParseException errors were observed in the pod logs for BSF Management service. **Doc Impact:** There is no doc impact.	3	25.1.100
38855968	Misconfiguration in BSF Management service with datasources.default.schema-generate=create_drop	It was identified that the `application.properties` file contained in `atasources.default.schema-generate=create_drop`. This setting caused the schema to be dropped and recreated upon each application startup, which could result in loss of all production data and service outages. The `datasources.default.schema-generate=create_drop` configuration was reviewed and changed to a safe value such as “none” to prevent the service outage and the data loss. **Doc Impact:** There is no doc impact.	3	25.2.200
38475917	REST API to delete all the pcfBinding sessions from database is not working	An attempt was made to delete all available PCF binding sessions from the database by using the `/oc-bsf-query/v1/pcfBindings/admin/databasecleanup` REST API. The request failed with the following error: "error":"Not Found","path":"/oc-bsf-query/v1/pcfBindings/admin/databasecleanup". **Doc Impact:** There is no doc impact.	3	25.2.100

Table 4-2 (Cont.) BSF 25.2.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
38380963	BSF_SERVICES_DOWN alert is updating as app-info service was down when scaling bsf-management pod to 0	The BSF_SERVICES_DOWN alert was updated to indicate that the app-info service was down when the bsf-management pod was scaled to 0. **Doc Impact:** The description of BSF_SERVICES_DOWN alert in BSF User Guide is changed from "{{$labels.microservice}} service is not running!" to "{{$labels.service}} service is not running!". For more information, see "BSF Alerts" section in *Oracle Communications Cloud Native Core, Binding Support Function User Guide*.	3	25.2.100
38648929	NullPointerException observed in CM service logs when changing log level for app-info service	When log level for app-info service was changed through CNC Console, a NullPointerException (NPE) was observed in the CM service logs, and a 500 Internal Server Error was displayed. **Doc Impact:** There is no doc impact.	3	25.2.200
38591830	Subscriber tracing "marker": {"name":"SUBSCRIBER"} is not observed in BSF revalidation message	Subscriber tracing marker {"name":"SUBSCRIBER"} was not observed on the bsf-revalidation message. **Doc Impact:** There is no doc impact.	3	25.2.100
38391474	Reconnection attempt from DSR to BSF does not happen when DPR has "BUSY" cause	When the Controlled Shutdown feature was enabled, BSF did not perform error mapping for Message Type: Disconnect-Peer-Request with Command Code: 282. During Controlled Shutdown execution, BSF sent a Disconnect-Peer-Request to DSR with the cause set to “BUSY” for an ongoing TCP and Diameter connection. **Doc Impact:** There is no doc impact.	3	24.2.2

Table 4-2 (Cont.) BSF 25.2.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
38705674	Unexpected "Request body has already been claimed: Two conflicting sites are trying to access the request body." error occurred in BSF Management service after upgrading to 25.2.200	During the in-service upgrade test, a few errors were observed related to the following message: "`Unexpected error occurred: Request body has already been claimed.`" **Doc Impact:** There is no doc impact.	3	25.2.200
38693223	BSF Management service is reporting "Error extracting UE ID from request body: No content to map due to end-of-input" error when both Enhanced logging and Enable UE Identifier is enabled	When Enhanced Logging and UE Identifier were enabled, BSF Management logs were flooded for every call. **Doc Impact:** There is no doc impact.	3	25.2.200
38934802	Remove unused Helm parameter isIpv6Enabled	The `isIpv6Enabled` parameter was deprecated and unused in Ingress Gateway, Egress Gateway, and Alternate-route services. Accordingly, these attributes were removed from the `custom-values.yaml` file to avoid confusion. **Doc Impact:** Removed "`isIpv6Enabled`" parameter from Customizing BSF section in *Oracle Communications Cloud Native Core, Binding Support Function Installation, Upgrade, and Fault Recovery Guide*.	3	25.2.200

Table 4-2 (Cont.) BSF 25.2.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
38963348	Reverting millisecond to second level precision for last_access_timestamp	Previously, last_access_timestamp values were updated with millisecond precision (for example, GREATEST(last_access_timestamp + 1, UNIX_TIMESTAMP(CURRENT_TIMESTAMP(3)) * 1000)) to improve conflict resolution and prevent duplicate timestamps during concurrent updates. This change aligned the column's precision with that of other services. However, multisite upgrade scenarios showed that upgraded sites stored timestamps in milliseconds, while non-upgraded sites continued to store timestamps in seconds. This discrepancy increased conflicts and introduced inconsistencies across sites, particularly during rolling or mixed-version upgrades. As a result, the millisecond-precision change was reverted to restore consistent behavior and compatibility across all environments. **Doc Impact:** There is no doc impact.	3	25.1.200
38729878	BSF Alertrule yaml file has extra space on namespace label	The BSF Alertrule yaml file had an extra space on the namespace label. **Doc Impact:** Updated the expression and description of the alerts for which the extra space is removed in the BSF_Alertrule.yaml file. For more details see, "BSF Alerts" section in *Oracle Communications Cloud Native Core, Binding Support Function User Guide*.	3	25.2.100

Table 4-2 (Cont.) BSF 25.2.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
38898693	Flooding of org.eclipse.jetty logs were observed in 25.2.200	The org.eclipse.jetty logs were flooded in BSF 25.2.200. **Doc Impact:** There is no doc impact.	3	25.2.200
38390051	Observed data inconsistency after completion of rollback	Data inconsistency was observed in the ocpm_bsf.pcf_binding table across two sites following completion of the rollback. A replication channel error was reported. The LOST_EVENTS incident occurred on the source. **Doc Impact:** There is no doc impact.	3	25.1.200
38940949	NRF Agent Import REST API with action=Create is successful, but configuration is not updated	The NRF Agent configuration import through REST API call with action=Create completed successfully, but the configuration was not updated. **Doc Impact:** There is no doc impact.	3	25.2.200
38365198	ocbsf-custom-values.yaml file does not expose containerPortNames parameter	The `custom-values.yaml` file for BSF 25.1.100 did not contain `containerPortName` parameter, which was used to provision backendPortName in the Cloud Native Load Balancer (CNLB) annotations. The `containerPortName` parameter was added to `custom-values.yaml` file to reduce the effort required to locate it in the charts. **Doc Impact:** There is no doc impact.	4	25.2.100
36866750	"Failed to update stats" (<class 'requests.exceptions.MissingSchema'>) error observed on Performance pods	The “Failed to update stats” error (<class 'requests.exceptions.MissingSchema'>) was observed on Performance pods. **Doc Impact:** There is no doc impact.	4	24.2.200

Table 4-2 (Cont.) BSF 25.2.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
38642472	Some of the configuration screens are not exported from CNC Console even when they are present on CNC Console	Certain configuration screens such as Perf-Info Logging Level, App-Info Logging Level, and Error Code Series List present in CNC Console are not exported when using the **Bulk Export** option. These screens are excluded from the exported output. This issue is observed in both freshly installed BSF deployments and upgraded environments (upgraded from 25.2.100 to 25.2.200). **Doc Impact:** There is no doc impact.	3	25.2.200

Note

Resolved bugs from 25.1.200 and 25.2.100 have been forward ported to Release 25.2.200.

4.2.3 cnDBTier Resolved Bugs

Release 25.2.201

Table 4-3 cnDBTier 25.2.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
38684514	API for changing preferredIpFamily from IPV4 to IPV6 and vice versa gives partial response on multi-channel setups	The API for changing the `preferredIpFamily` in dual stack setups (from IPv4 to IPv6 or vice versa) did not return a detailed JSON response for multi-channel configurations. Instead of listing all replication channel groups configured for the local site, the API response returned a randomly selected replication channel group per remote site. **Doc impact**: Updated the "Support for Dual Stack" section in *Oracle Communications Cloud Native Core, cnDBTier User Guide*.	2	25.1.201

Table 4-3 (Cont.) cnDBTier 25.2.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
38671447	Replication service resolves to IPv6 IP instead of FQDN, causing TLS SAN mismatch and connection failures	The replication microservice used a raw IPv6 address instead of the configured FQDN to connect to remote sites, causing TLS validation failures due to certificate SANs containing only FQDNs. This led to REST API call failures, repeated communication errors in the logs, and prevented replication from initializing. **Doc impact**: Updated the "Support for Dual Stack" section in *Oracle Communications Cloud Native Core, cnDBTier User Guide*.	2	25.1.201

Table 4-3 (Cont.) cnDBTier 25.2.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
38567831	SLF DBTier Recover script is failing during migration to new site	While migrating to a new site, the SLF DBTier Recover script failed to run successfully. The migration process included uninstalling the previous site, cleaning up related database entries, upgrading existing sites, and configuring the new site on an updated cluster. However, due to communication issues between the new and existing sites, the recovery script was unable to complete, resulting in a failed migration scenario. **Doc impact**: Updated the "Removing a Georedundant cnDBTier Cluster" section in *Oracle Communications Cloud Native Core, cnDBTier User Guide*.	2	25.1.201

Table 4-3 (Cont.) cnDBTier 25.2.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
38385887	During BT Data/ Voice Call Model performance test, mysql-cluster-db-backup-manager-svc pod restart has been observed unexpectedly	During high-load performance testing on a multi-site cluster, repeated restarts of a subset of `ndbappmysqld` pods on one site resulted in the unexpected restart of the `mysql-cluster-db-backup-manager-svc` pod. This behavior highlights a potential stability issue where ongoing disruptions to `ndbappmysqld` pods can impact the reliability of backup operations managed by the `mysql-cluster-db-backup-manager-svc` pod, especially during periods of system stress or failover scenarios. **Doc impact**: There is no doc impact.	2	25.2.100

Table 4-3 (Cont.) cnDBTier 25.2.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
38677062	SLF dbtremovesite is restarting the application pods	When running the `dbtremovesite` script as part of a site removal or migration process in a multi-site SLF environment, it was observed that running the script caused unexpected restarts of system services—specifically, the monitor-service and backup-manager-svc pods. These restarts further triggered associated application pods to restart, even though the active sites were handling live traffic. This unexpected pod behavior is not aligned with the intended function of the script, as standard removal procedures do not require disruption to application services on active sites. **Doc impact**: There is no doc impact.	2	25.1.100
38284918	Down site local backup during non-fatal GRR status changed from COMPLETED to FAILED in backup-manager-svc pod log	Check if backup is completed successfully before dropping the databases during the GRR. **Doc impact**: There is no doc impact.	3	25.1.200

Table 4-3 (Cont.) cnDBTier 25.2.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
38181539	REPLICATION_DOWN alert falsely triggers due to missing metrics during prometheus scrapes	Replication failed Alert Logic to be fired on an actual switch over and not on Metrics Missing Cases. **Doc impact**: There is no doc impact.	3	23.4.3
38582579	Rest API of db-replication-svc will not be accessible outside db-replication-svc during migration of http	During migration from HTTPS to HTTP or vice versa, the REST API of `db-replication-svc` becomes inaccessible outside the service due to a configuration mismatch. As a result, while `db-replication-svc` expects HTTPS connections, client services such as `monitor-svc` and `helm test` perceive HTTPS as disabled and attempt to connect over HTTP. This mismatch in protocol configuration leads to failed REST API calls during the initial handshake, resulting in observed errors and disrupted communication during the migration process. **Doc impact**: There is no doc impact.	3	25.2.100

Table 4-3 (Cont.) cnDBTier 25.2.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
38487200	Remove export of DBTIER_RELEASE_NAME in horizontal scaling procedure using dbtscale_ndbmtd_pods	The horizontal scaling procedure for `ndbmtd` pods previously required users to manually export the `DBTIER_RELEASE_NAME` environment variable before running the `dbtscale_ndbmtd_pods` script. With this fix , this manual export is no longer necessary. As a result, the step to manually export `DBTIER_RELEASE_NAME` had to be removed from the horizontal scaling documentation to reflect the updated process. **Doc impact**: Updated the "Horizontal Scaling of ndbmtd pods using dbtscale_ndbmtd_pods" section to remove the export `DBTIER_RELEASE_NAME` command. For more information, see Oracle Communications Cloud Native Core, cnDBTier User Guide.	3	25.2.100

Table 4-3 (Cont.) cnDBTier 25.2.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
38637939	Documentation error in "Remove cnDBTier Geo-Redundant Site" procedure	The documentation should be updated to ensure the reference log aligns with the intended removal of cluster1. **Doc impact**: Updated Step 4 of "Remove cnDBTier Geo-Redundant Site" procedure in *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide.*	3	25.2.101
38646497	25.1.201-1 : Observing outbound traffic on ipv4	Outbound traffic from the DB replication service was observed using IPv4, even though IPv6 was configured as the preferred protocol in the service settings. This occurred despite internal and most external services being set to use IPv6, with only optional dual-stack fallback. **Doc impact**: There is no doc impact.	3	25.1.201

Table 4-3 (Cont.) cnDBTier 25.2.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
38648664	GRR API for marking remotesite as failed giving OK response for unconfigured remotesite	The GRR API for marking a remotesite as failed was returning a 200 OK response even when the specified remotesite was not configured in the setup. The API indicated a successful operation regardless of the existence or configuration status of the remotesite which was incorrect. **Doc impact**: There is no doc impact.	3	25.2.101
38652957	Real Time Replication Status shows incorrect status of replication when one replication channel is down between 2 sites	In a 4-site multichannel setup, the system reported the overall replication status as UP for a site even when one or more replication channels between sites were down. The API did not evaluate or display replication status on a per-channel basis, resulting in a misleading aggregate site-level status that indicated healthy replication despite individual channel failures. **Doc impact**: There is no doc impact.	3	25.2.100

Table 4-3 (Cont.) cnDBTier 25.2.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
38660810	Real Time Replication Status API responds incorrect Error Code When Monitor Service cannot communicate with all SQL pods on a site	The Real Time Replication Status API returned a 500 Internal Server Error or timed out whenever the monitor service lost communication with all SQL pods on Site 1, rather than returning the expected 503 Service Unavailable status code. This incorrect error code can mislead clients into interpreting the issue as a server malfunction instead of a temporary service unavailability. **Doc impact**: There is no doc impact.	3	25.2.100
38660862	New Real Time Replication Status REST API Returns 200 Instead of 503 when Communication breaks between Monitor service and Replication services(1 or more) on Site 1	The new Real Time Replication Status REST API returned a 200 OK status code even when there was a communication failure between the monitor service and one or more replication services on Site 1. In these cases, the response showed `allSqlStatusDetails = null` for the affected replication service, instead of returning a 503 Service Unavailable error. **Doc impact**: There is no doc impact.	3	25.2.100

Table 4-3 (Cont.) cnDBTier 25.2.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
38669677	Real Time Replication Status API Only Reports Local Site Replication Status and Fails to Return Replication Details for Remote Sites	The Real Time Replication Status API returned replication status only for the local (requesting) site, omitting replication details for remote sites in the cluster. **Doc impact**: There is no doc impact.	3	25.2.100
38660967	Real Time Replication Status returns 502 or Timeout Instead of 400/404 when Monitor Service is down	When the Monitor service is down, the Real-Time Replication Status API returns a 502 Bad Gateway error or times out, rather than providing a clear and appropriate 400 or 404 error response. This incorrect status handling lead to misleading client behavior and prevented accurate identification of the monitor's unavailability. **Doc impact**: There is no doc impact.	3	25.2.100

Table 4-3 (Cont.) cnDBTier 25.2.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
38651597	cnDBtier Replication Service leader Pod is not coming up and taking some time	During fresh installation in a multi-site environment, the Replication Service leader pod did not come up promptly when other sites in the cluster were not yet installed. The pod only started successfully after installation progressed on additional sites. Investigation found that this delay was related to certain service containers being unhealthy during the initial startup phase, resulting in extended initialization times for the leader pod. **Doc impact**: There is no doc impact.	3	25.1.201
38685798	dbtreplmgr prints http connection on HTTPS TLS enabled setup	When running the `dbtreplmgr` script on a setup with HTTPS and TLS enabled, the script output incorrectly indicated HTTP connections in the logs, even though the environment was configured for secure HTTPS communication. This misrepresentation in the script output can cause confusion and does not accurately reflect the actual security protocol in use. **Doc impact**: There is no doc impact.	3	25.1.201

Table 4-3 (Cont.) cnDBTier 25.2.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
38685274	Continuous ERROR logs being printed in db-monitor-svc	After upgrading a 3-site, 2-channel setup with HTTPS and TLS enabled from 25.1.201-2 to 25.1.201-3, continuous ERROR logs are being generated in `db-monitor-svc` indicating "[DbtierRetrieveBackupTransferMetrics] No Backups Transfers Started to provide the Backup Status Metrics." These log messages are appearing at a frequency of approximately once per minute, despite the GRR operation completing successfully on the sites. **Doc impact**: There is no doc impact.	3	25.1.201
38710352	Update required in output of dbtscale_ndbmtd_pods in phase zero(0)	When running the `dbtscale_ndbmtd_pods` script in Phase 0 on a 3-site, 3-channel ASM-enabled setup configured for dual stack with IPv6 preferred, the script output displayed usage of IPv4 for internal operations. This is inconsistent with the deployment's configured IPv6-preferred protocol and may lead to confusion or misinterpretation during scaling activities. **Doc impact**: There is no doc impact.	3	25.2.101

Table 4-3 (Cont.) cnDBTier 25.2.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
38710401	Update required in output of dbtreplmgr in phase zero(0)	When running the `dbtreplmgr` script in Phase 0 on a 3-site, 3-channel ASM-enabled setup configured for dual stack with IPv6 preferred, the script output indicated usage of IPv4 for internal operations. This behavior is inconsistent with the deployment's preferred IPv6 configuration and may cause confusion during initial setup and verification. **Doc impact**: There is no doc impact.	3	25.2.101
38710531	Update required in output of dbtscale_vertical_pvc in phase zero(0)	During vertical scaling operations using the scaling script, it was observed that the script defaulted to using IPv4 for internal processes, even though the environment was configured for dual stack with IPv6 as the preferred protocol. **Doc impact**: There is no doc impact.	3	25.2.101

Table 4-3 (Cont.) cnDBTier 25.2.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
38631076	CNDB- Pending GRR should fail if it stucked for longer duration	Pending Georeplication Recovery operations did not automatically fail when they remained unprogressed for an extended period. During upgrade and rollback procedures in a multi-site environment, it was observed that a GRR process stayed stuck in a pending state for over 12 hours without progressing or timing out. **Doc impact**: There is no doc impact.	3	25.1.103
38724990	DBTIER 25.1.201 : DBtier Installation Guide does not have Post upgrade checks related to schema	cnDBTier documentation did not include procedures or checks to verify that the database schema has been correctly upgraded and that the upgrade was fully successful. **Doc impact:** A new section has been added to verify if the database schema upgrade has completed successfully on any site. For more information, see *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide.*	3	25.1.201

Table 4-3 (Cont.) cnDBTier 25.2.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
38768457	Inconsistent Replication Status Between Realtime Replication APIs When DB-Monitor to Replication Service Communication Is Broken	An inconsistency was observed between the cluster-level and site-specific replication realtime status APIs when communication between the db-monitor service and a replication service was disrupted. In such cases, the cluster-level API reported the replication status between sites as DOWN, while the site-specific API reported it as UP. Both APIs are expected to provide consistent status reporting. **Doc impact**: There is no doc impact.	3	25.2.101

Table 4-3 (Cont.) cnDBTier 25.2.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
38818934	Wrong Rest URL mentioned in DBTier Status API section in 25.2.200 User Guide	The DBTier Status API section in the 25.2.200 User Guide listed an incorrect REST URL: `http://base-uri/db-tier/db-tier/replication/status/realtime`. **Doc impact**: The *cnDBTier Status API* section has been updated to reflect the correct URL: `http://base-uri/db-tier/replication/status/realtime`. For more information, see *Oracle Communications Cloud Native Core, cnDBTier User Guide.*	3	25.2.101

Table 4-3 (Cont.) cnDBTier 25.2.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
38855643	BSF 25.2.101 replication down after upgrade	After upgrading the BSF application and cnDBTier (from 25.1.100/25.1.103 to 25.2.101) across three sites in a GR setup, replication from Site 3 to Site 2 failed. Logs indicated an "Unknown database" error for `bsf_ocbsf_overload`, which was missing on Site 3 but present on Site 1 and Site 2. The issue was first observed after upgrading Site 2's cnDBTier. All database privileges were confirmed to be correct, and pre-upgrade health checks reported no missing tables. **Doc impact**: There is no doc impact.	3	25.2.101

Table 4-3 (Cont.) cnDBTier 25.2.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
38865774	Metrics are getting missed on site-3 on a 3 site GR Setup - 6 replication group	In a 3-site GR setup with 6 replication groups (IPv6), metrics for certain nodes (e.g., node_id 56 and 57) are not being reported on the Grafana dashboard—even though traffic on these nodes is running and replication is functioning correctly. Specifically, metrics such as `db_tier_api_bytes_sent_count` and `db_tier_api_wait_exec_complete_count` are missing for the affected nodes, indicating a gap in metric collection or reporting despite normal data and replication activity. **Doc impact**: There is no doc impact.	3	25.1.201
38971451	binlog purge errors observed during a long duration PCF performance run	During a long-duration PCF performance run, the replication SQL pods intermittently logged “Bin Log Sizes Empty at the local site” while running scheduled binlog purge checks.. **Doc impact**: There is no doc impact.	3	25.1.201

Table 4-3 (Cont.) cnDBTier 25.2.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
38894669	Site Specific PCF DB GRANTS not being replicated across sites using MultiRep Channels	In multi-site deployments using MultiRep channels, site-specific database users and GRANTs were intermittently replicated across sites, resulting in inconsistent permissions between sites. **Doc impact**: Added the section "Mandatory Guidelines for User and Grant Operations" to provide mandatory guidelines for schema, user, and grant operations. For more information, see *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide.*	3	25.1.200

Table 4-3 (Cont.) cnDBTier 25.2.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
38958827	Request for Documentation and Audit Script PCF NF SKIP ERROR Configuration	Documentation for PCF NF replication SKIP ERROR configuration covering recommended skip-error threshold values per NF nor the referenced database audit script was not available. **Doc impact**: cnDBTier documentation was updated to include the section "cnDBTier Replication Skip Errors" that provided information on replication skip errors as part of its replication error-handling mechanism when applying epochs between sites. For more information, see *Oracle Communications Cloud Native Core, cnDBTier User Guide.*	3	24.2.1
38717425	DBTier: Unsupported characters in backup encryption password	Backup and restore operations were failing due to the use of unsupported characters in the backup encryption password. The system allowed passwords containing characters outside the permitted set leading to failures during backup and recovery. **Doc impact**: There is no doc impact.	4	24.2.6

> **Note**
>
> Resolved bugs from 25.1.100, 25.1.201, and 25.2.101 have been forward ported to release 25.2.201.

4.2.4 CNC Console Resolved Bugs

Release 25.2.200

Table 4-4 CNC Console 25.2.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38319858	POLICY_READ Role enabled but user is also able to edit the parameters	Users who only had the POLICY_READ role assigned were able to edit parameters on some Policy screens. The "General Configurations" screen correctly blocked write operations with a "403 FORBIDDEN" error, but the "policy-project" screen allowed users to save changes. This happened because the Policy API prefix was not added on certain screens. **Doc Impact:** There is no documentation impact.	3	24.2.3
38528957	CNC Console Logs concerns/ requests	CNC Console log data issues such as missing login error logs, events logged at the DEBUG level instead of WARNING or INFO, lack of audit or security attributes, and incomplete metadata for some resource access logs were reported. Some activities, such as failed logins, were not generating expected Splunk events, and fields like AuthenticationType were set to unknown. **Doc Impact:** The "Logs" section in *Oracle Communications Cloud Native Configuration Console Troubleshooting Guide* has been updated to include additional NF (BSF, POLICY, SCP etc.,) SECURITY and AUDIT log examples.	4	23.4.1

Table 4-4 (Cont.) CNC Console 25.2.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38524240	Format Issues identified from Security CNCC Log Analysis	Log messages were not in standard JSON format, and several attributes contained placeholders instead of values. Header, and payload fields were also formatted as custom key or value pairs, not JSON. **Doc Impact:** All logs in the "Logs" section of *Oracle Communications Cloud Native Configuration Console Troubleshooting Guide* have been standardized to use JSON format for the message, headers, and payload fields, and placeholders have been removed. The log message label has been corrected to populate as a JSON object by default.	4	23.4.1
38753758	CNCC installation is failing in Openshift 4.14	If a user updated the *runAsUser* field in the *securityContext* of a pod or container to use an arbitrary user ID instead of the default hardcoded value, the iam-kc pod entered a CrashLoopBackOff state. To resolve this issue, the IAM Dockerfile was updated to support the use of arbitrary user IDs as specified in the *runAsUser* field. **Doc Impact:** There is no documentation impact.	3	25.2.100

4.2.5 CNE Resolved Bugs

Release 25.2.200

There are no resolved bugs in this release.

> **Note**
>
> Resolved bugs from 25.2.1xx have been forward ported to Release 25.2.200.

4.2.6 NSSF Resolved Bugs

Release 25.2.200

Table 4-5 NSSF 25.2.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38307293	NSSF - Missing max concurrent streams on ingress gateway	The NSSF ingress gateway did not populate the `serverDefaultSettingsMaxConcurrentStream` value in the HTTP/2 settings, so HTTP/2 clients treated the maximum concurrent streams as 1, which caused a traffic bottleneck. **Doc impact:** There is no doc impact.	2	25.1.100
38159590	[25.1.200] Multiple instances of restart for ns-selection pods were observed over a run of 18 hr with reset stream (Running 7K success and 3.5K failure as part of http reset stream on Site1)	The ns-selection pods restarted multiple times during an 18-hour run when HTTP/2 reset stream traffic was sent. This occurred in a three-site GR setup with traffic on Site1, where 10.5K TPS included 7K successful requests and 3.5K reset stream requests. **Doc impact:** There is no doc impact.	2	25.1.200
38716716	Need 25.1.100 - Unexpected behavior for NSSF nrf-client when scaled to zero	When you scaled the NSSF nrf-client pod to zero, the NSSF NF registration status in NRF was inconsistent: it sometimes changed to **SUSPENDED** but sometimes was **DEREGISTERED**. This behavior occurred when the nrf-client received the **Deregistration** status from app-info during termination and sent a DELETE request to NRF. In 25.2.200, nrf-client was removed as a critical service in app-info by updating the custom values YAML, which prevented deregistration when nrf-client was scaled down. **Doc impact:** There is no doc impact.	3	25.1.100

Table 4-5 (Cont.) NSSF 25.2.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38341986	NSSF ATS 25.1.100: NRF Stub Server Returning Internal Error (500)	An Automated Test Suite scenario failed when two NRF stub servers were configured to return 503 and the third stub server was expected to return a successful 20x response, but it returned a 500 internal error. As a result, all NRF stub servers were marked as UNHEALTHY and the expected `nnrf-disc` message was not sent to NRF, and the test failed with "No Healthy NRF Routes available, cannot send Request." **Doc impact:** There is no doc impact.	3	25.1.100
38125454	NSSF ATS 25.1.100 MultiplePLMN Feature failing because expiry parameter set to statically.	NSSF ATS regression test cases for the MultiplePLMN feature failed because the request files contained a statically set `expiry` value (for example, `2025-06-25T09:23:45.123456Z`). NSSF returned `HTTP/2 400 Bad Request` with `OPTIONAL_IE_INCORRECT` and `detail: 'Bad Request. Wrong duration'`. **Doc impact:** There is no doc impact.	3	25.1.100
38545826	NSSF 25.1.200 Expired subscriptions: The database is not cleaning after subscription	NSSF continued to send notifications to AMFs for subscriptions that had already expired, and the expired subscription records were not purged from the database until 24 hours after creation. **Doc impact:** There is no doc impact.	3	25.1.200

Table 4-5 (Cont.) NSSF 25.2.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38500020	NSSF 25.1.200 : Documentation for few features missing in NSSF GUI	The NSSF GUI did not include documentation links for several regression feature files, including `Delete_NssfEventSubscription.feature`. **Doc impact:** Updated the "Configuring NSSF using CNC Console" section in "*Oracle Communications Cloud Native Core, Network Slice Selection Function User Guide*".	3	25.1.200
38753670	NSSF install failing on Openshift 4.14	NSSF installation on OpenShift 4.14 failed because OpenShift blocked pod creation when the pods used a fixed `runAsUser` value that was outside the namespace UID range, and the preinstall hook failed to start when it tried to create temporary files under `/tmp` on a read-only file system. **Doc impact:** There is no doc impact.	3	25.1.200
38192130	25.1.200: [Incorrect response code in case of expired token is sent in request]	When you sent a request with an expired token, NSSF returned HTTP status **408** with `WWW-Authenticate: ... error="invalid_token"` instead of returning **401** for `invalid_token`. **Doc impact:** There is no doc impact.	3	25.1.200
38219417	NSSF 25.1.200 Discrepancies in Alert Names Between User Guide and Rule Files	Alert names in the user guide did not match the alert rule YAML file, and one alert appeared only in the user guide. **Doc impact:** Updated the "NSSF Alerts " section in "*Oracle Communications Cloud Native Core, Network Slice Selection Function User Guide*".	3	25.1.200

Table 4-5 (Cont.) NSSF 25.2.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37966602	NSSF is compressing the response when response size is less than 1024 Bytes for an availability PUT request, when gzip compression is enabled	When gzip compression was enabled, NSSF compressed responses to availability PUT requests even when the response size was less than 1024 bytes. **Doc impact:** There is no doc impact.	3	25.1.100
37966541	NSSF is not able to handle avail request when Payload is more than 1 MB and gzip feature is enable	When you sent an availability PUT request with a payload larger than 1 MB while gzip compression was enabled, NSSF returned an HTTP request timeout instead of returning 413 `Request Entity Too Large`. **Doc impact:** There is no doc impact.	3	25.1.100
37639879	oauth failure is not coming in oc_ingressgateway_http_responses_total metrics	When you sent traffic with invalid OAuth access tokens, the OAuth failure responses were not counted in the `oc_ingressgateway_http_responses_total` metric even though they were counted in `oc_oauth_validation_failure_total`. **Doc impact:** There is no doc impact.	3	25.1.100
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	When you enabled empty frames in all ns-selection and ns-availability requests and ran 10.5K traffic, NSSF rejected ns-selection traffic and dropped 0.045% of requests with HTTP 503 errors. **Doc impact:** There is no doc impact.	3	25.1.100
37048499	GR replication is breaking post rollback to of CNDB 24.2.1	CNDB replication failed after you rolled back from 24.3.0-rc.1 to 24.2.1-rc.4 in a two-site GR setup. Replication went down after the second site rollback completed and the first site rollback finished. **Doc impact:** There is no doc impact.	3	24.3.0

Table 4-5 (Cont.) NSSF 25.2.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37303227	[NSSF 24.3.0] [EGW-Oauth feature] "Oc-Access-Token-Request-Info:" IE should not come in notification.	When you enabled OAuth token requests for subscription notifications, NSSF included the `Oc-Access-Token-Request-Info` header in notification messages. **Doc impact:** There is no doc impact.	3	24.3.0
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.	During a PDU session establishment test with 9K TPS for slices configured in the database and 1K TPS for slices not configured in the database, NSSF returned incorrect results. NSSF returned successful responses for 0.4% of requests for slices that were not configured, and it returned 403 and 503 errors for some requests for slices that were configured. **Doc impact:** There is no doc impact.	3	24.3.0
36285762	After restarting the NSselection pod, NSSF is transmitting an inaccurate NF Level value to ZERO percentage.	After you restarted the ns-selection pod, NSSF reported an incorrect NF-level load of 0% in the `/load` response and in the `3gpp-Sbi-Lci` header, even though the NF-service-instance load value was nonzero (for example, 29%). **Doc impact:** There is no doc impact.	3	23.4.0
35888411	Wrong peer health status is coming "DNS SRV Based Selection of SCP in NSSF"	When peer monitoring was enabled and DNS SRV selection was disabled, the peer health status reported an invalid SCP IP address as healthy and did not report health status for the peer configured through a virtual host. **Doc impact:** There is no doc impact.	3	23.3.0

Table 4-5 (Cont.) NSSF 25.2.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38857519	NSSF 25.1.200 - Duplicated key: port in the ingress-gateway section of default CV	The default NSSF custom values file defined the `ports` key twice in the ingress-gateway section, which could cause exceptions in external tools that generate custom values files. **Doc impact:** There is no doc impact.	4	25.1.200
37323951	prometheus url comment should be mentioned overload and LCI/OCI feature in NSSF CV file	The comment for the Prometheus URL in the NSSF custom values file stated that the URL was mandatory only for the LCI/OCI feature, even though it was also required for the Overload feature. **Doc impact:** There is no doc impact.	4	24.3.0
37622760	NSSF should send 415 responses to ns-selection and ns-availability requests if their content type is invalid.	When you sent ns-selection or ns-availability requests with an invalid `Content-Type` header (for example, `multipart/form-data`), NSSF returned a 500 error instead of returning 415 `Unsupported Media Type`. **Doc impact:** There is no doc impact.	4	25.1.100
37617910	Subscription Patch should be a part of Availability Sub Success (2xx) % panel in Grafana Dashboard	The Grafana **Availability Sub Success (2xx) %** panel did not include subscription PATCH results, so subscription patch failures (such as 405 errors) were not shown in the service status view. **Doc impact:** There is no doc impact.	4	25.1.100

Table 4-5 (Cont.) NSSF 25.2.200 Resolved Bugs

Bug Number	Title	Description	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".	When you sent ns-selection and ns-availability requests with an invalid `Accept` header, NSSF returned 404 responses for subscription delete and subscription patch requests instead of returning a 406 Not Acceptable response with a “No acceptable representation” detail. **Doc impact:** There is no doc impact.	4	25.1.100
37612743	If URLs for ns-selection and ns-availability are invalid, NSSF should return a 404 error code and title with INVALID_URI.	When you sent ns-selection and ns-availability requests with an invalid URL, NSSF returned inconsistent errors: the ingress gateway returned 404 when the request used an incorrect microservice address, but NSSF returned 400 with `title` set to `INVALID_URI` when the request reached NSSF with an incorrect endpoint. **Doc impact:** There is no doc impact.	4	25.1.100
36881883	In Grafana, Service Status Panel is showing more than 100% for Ns-Selection and Ns-Avaliability Data	The Grafana Service Status panel showed percentages greater than 100% for ns-selection and ns-availability data. **Doc impact:** There is no doc impact.	4	24.2.0

4.2.7 OSO Resolved Bugs

Release 25.2.200

There are no resolved bugs in this release.

> **Note**
>
> Resolved bugs from 25.2.1xx have been forward ported to Release 25.2.200.

4.2.8 OCCM Resolved Bugs

Release 25.2.200

There are no resolved bugs in this release.

4.2.9 Common Services Resolved Bugs

4.2.9.1 Egress Gateway Resolved Bugs

Release 25.2.108

Table 4-6 Egress Gateway 25.2.108 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
38957729	EGW is not able to send access token request towards NRF in TLS enabled setup	In TLS-enabled deployments with OAuth enabled, Egress Gateway failed to send access-token requests to the NRF because it could not establish a TLS connection, causing call failures.	2	25.1.208
38894990	PCF EGW not giving precedence to IPV6 and resolving to IPV4 address	Istio logs showed that PCF resolved an NRF host name to a downstream local IPv4 address when it should have resolved to an IPv6 address.	3	25.1.203
38569278	Ingress Gateway reports a NullPointerException after the installation of PCF	After PCF is installed, Ingress Gateway pods reported a `NullPointerException` when they started.	3	25.2.108

> **Note**
>
> Resolved bugs from 25.2.1xx have been forward ported to Release 25.2.108.

Release 25.2.107

Table 4-7 Egress Gateway 25.2.107 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
38777247	PCF using expired token (25.2.107)	PCF intermittently used an expired token, which caused calls to fail.	2	25.1.200

Table 4-7 (Cont.) Egress Gateway 25.2.107 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
38795596	During EGW Upgrade from 25.1.203 to 25.2.106 Observed "java.io.InvalidClassException " on new 25.2.106 egw pods and No traffic drop observed	During an Egress Gateway upgrade from 25.1.203 to 25.2.106, the new Egress Gateway 25.2.106 pods reported a `java.io.InvalidClassException`, and no traffic drop was observed.	3	25.2.106

> **Note**
>
> Resolved bugs from 25.2.1xx have been forward ported to Release 25.2.107.

Release 25.2.106

Table 4-8 Egress Gateway 25.2.106 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
38661262	HealthStatus/peerSet GET, giving 500, NULL POINTER EXCEPTION in response	A GET request to the `/egw/healthStatus/peerSet` endpoint could have returned HTTP 500 with a NullPointerException when peer monitoring was enabled and peer/peerset/route configuration was present.	2	25.2.106
38704688	EGW peer health status is inconsistent in case of multiple EGW pods in IPv6 with a synchronization delay of ~>=1min	In IPv6 deployments with multiple Egress Gateway replicas and peer monitoring enabled, peer health could have been reported inconsistently across pods (some pods marking a peer healthy while others marked it unhealthy), leading to intermittent call failures when an unhealthy peer was selected.	2	25.1.207
38702789	Peer health ping request timing out after fresh install/ upgrade in IPv6	In dual stack IPv6 mode, Egress Gateway peer health pings to `/health/v3` could time out after a fresh installation or upgrade, marking all peers unhealthy and causing call failures.	2	25.1.207

Table 4-8 (Cont.) Egress Gateway 25.2.106 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
38719525	peer health status is showing incorrect peer scheme for https peer in EGW 25.2.105 build	The Egress Gateway peer health status output could have displayed an incorrect peer scheme for peers configured to use HTTPS when TLS was enabled.	2	25.2.105
37914904	Required Grafana dashboard JSON containing all the metrics for PI-B-25 PoP25 feature (IGW+EGW) along with Traffic success	The provided Grafana dashboard JSON for Egress Gateway and Ingress Gateway metrics set was missing Egress Gateway traffic success panel, resulting in incomplete visibility for traffic success.	4	25.1.200
38324716	Mounting of secrets is not backward compatible approach	After secrets were changed to be volume mounted for TLS 1.3 support on Kubernetes, updating or adding a new secret (for example, for CCA-related configuration) could have required a Helm upgrade to include the new secret in the mount list, unlike earlier behavior.	3	25.1.200
38235950	NPE seen in egress gateway after pod restart	After restarting Egress Gateway pods, Egress Gateway could have thrown a NullPointerException during startup, observed across all Egress Gateway pods.	3	25.2.100
38325304	cgiu_jetty_ip_address_fetch_failure metric name shall starts with oc rather cgiu	The `cgiu_jetty_ip_address_fetch_failure` metric name did not follow the standard `oc_` prefix naming convention and used a nonstandard prefix.	3	25.1.200

Note

Resolved bugs from 25.1.1xx and 25.2.1xx have been forward ported to Release 25.2.106.

4.2.9.2 Ingress Gateway Resolved Bugs

Release 25.2.108

Table 4-9 Ingress Gateway 25.2.108 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
38921131	When OC discards OverloadControlFilter attempts to update internal metrics using a null key or value, resulting in a NullPointerException in ConcurrentHashMap.put()	Overload Control discarded attempts by OverloadControlFilter to update internal metrics with a null key or value, and this resulted in a NullPointerException in `ConcurrentHashMap.put()`.	2	25.2.107
38831358	Non-ASM: Memory leak observed in IGW Non-ASM set-up with 12k traffic, resulting IGW pod restarts after 7days of continuous run	A memory leak was observed in an Ingress Gateway non-ASM setup with 12K traffic.	2	25.2.106
38861854	Increase of failure rate % after in-service upgrade to 24.2.4 and to 25.1.202	Ingress Gateway failure rate increased after an in-service upgrade to 24.2.4 and to 25.1.202.	2	24.2.13
38787849	New "tokenCacheSize" boundary value validation is not happening even though fresh install/upgrade is success	In Gateway Services 25.2.106, ASM did not validate the boundary value for the new `tokenCacheSize` attribute even though the fresh installation or upgrade succeeded.	3	25.2.106
38470214	"occnp_oc_ingressgateway_http_responses_total" metric not getting incremented	After the configuration of SBI Ingress Error Mapping for a controlled shutdown of PCF, 503 responses were not recorded in the `occnp_oc_ingressgateway_http_responses_total` metric.	3	24.2.7
38569278	Ingress Gateway reports a NullPointerException after the installation of PCF	After PCF is installed, Ingress Gateway pods reported a `NullPointerException` when they started.	3	25.2.108
38867575	Issue - Metric oc_oauth_validation_failure_total with invalid-scope dimension not pegged	During the UDR regression suite, the `oc_oauth_validation_failure_total` metric was not getting pegged for the specified curl request.	3	25.2.107

> **Note**
>
> Resolved bugs from 25.2.1xx have been forward ported to Release 25.2.108.

Release 25.2.107

Table 4-10 Ingress Gateway 25.2.107 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
38702154	After 1.5hrs run Continuous IRC are flooding in IGW when IGW freshly installed & Traffic loss is observed from 3K to 1.7K	In ASM, after 1.5 hours of continuous run, Illegal Reference Count (IRC) messages surged in Ingress Gateway after a fresh Ingress Gateway installation, and traffic dropped from 3K to 1.7K.	1	25.1.207
38767321	NPE and 500 internal ERROR observed in the POP25 error code rejections with configurable ERROR code	A `NullPointerException` and a 500 internal error occurred during pod protection error code rejections when a configurable error code was used.	2	25.2.106
38818360	helm install is failing with execution error at "custom-header.tpl:3:3): defaultVal is null" and same working fine in the 25.1.207 build	The Helm installation failed with the execution error `custom-header.tpl:3:3): defaultVal is null`, even though it worked in Gateway Services 25.1.207.	2	25.2.106
38787849	New "tokenCacheSize" boundary value validation is not happening even though fresh install/upgrade is success	The new `tokenCacheSize` boundary value validation did not occur even though the fresh installation or upgrade succeeded.	3	25.2.106

> **Note**
>
> Resolved bugs from 25.2.1xx have been forward ported to Release 25.2.107.

Release 25.2.106

Table 4-11 Ingress Gateway 25.2.106 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
38293029	High CPU utilisation was observed when OAuth feature is enabled with ASM	When the OAuth feature was enabled with ASM, Gateway Services could have shown elevated CPU utilization (about 10% higher than a baseline configuration) during performance testing.	3	25.2.100
38665926	allowedClockSkewSeconds IE value is wrongly configured in values.yaml file for IGW	The sample `values.yaml` for Ingress Gateway OAuth configuration could have specified `allowedClockSkewSeconds` as `1L`, which caused Ingress Gateway to interpret the value as `0` at runtime.	2	25.2.106
38369251	observed "Service MapDistCache has been terminated" in the old IGW pod after that new pods are not coming up when some of the IGW pods are deleted	Under heavy traffic and after partial pod restarts, Ingress Gateway pods could fail to come up after some replicas were removed, with logs showing “Service MapDistCache has been terminated,” which prevented new pods from taking traffic.	3	25.2.100
38468707	IGW continues discarding discovery requests after overload trigger during ISSU, despite receiving normal load level signals	During ISSU scenarios, Ingress Gateway could have continued discarding discovery requests after overload protection was triggered, even after new pods reported a normal load level, and the condition did not self-recover without restarting pods.	3	25.1.205
38272205	fillrate accepting zero value and IGW pod is restarting continuously when the pop feature is disabled	When the Pod Protection feature was disabled, Ingress Gateway could have accepted a `fillrate` value of `0` (despite validation requiring a positive value when the feature was enabled), which led to a divide-by-zero during policer initialization and caused the pod to restart continuously.	3	25.1.200

Table 4-11 (Cont.) Ingress Gateway 25.2.106 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
38148295	Some of the pod protection parameters validation happening with and without flag enabled. all parameters are not in sync.	Some pod protection configuration parameters, for example, congestion and deniedAction, could have been validated even when the pod protection feature flag was not enabled, resulting in inconsistent validation behavior across parameters.	4	25.1.200
36089938	errorcodeserieslist api allows configuration of errorCodeSeries having errorSet with no errorCodes	The validation logic in the errorcodeserieslist API only checked whether errorCodeSeries and errorCodes were null, but did not verify if these fields were empty arrays.	3	23.4.0

> **Note**
>
> Resolved bugs from 25.1.1xx and 25.2.1xx have been forward ported to Release 25.2.106.

4.2.9.3 Alternate Route Service Resolved Bugs

Release 25.2.108

Table 4-12 Alternate Route Service 25.2.108 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
38594342	Alternate Route Service reports a NullPointerException after the installation of PCF	Alternate Route Service reported NullPointerException after the installation of PCF.	3	25.2.200

> **Note**
>
> Resolved bugs from 24.2.x and 25.2.1xx have been forward ported to Release 25.2.108.

Release 25.2.107

Table 4-13 Alternate Route Service 25.2.107 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
38828633	Scheme change for the same host:port was not handled correctly during concurrent updates	When an update (Deletion) was received for HTTPS SRV records, the system removed all existing entries for the same vFQDN, including those associated with HTTP.	3	23.4.106

> **Note**
>
> Resolved bugs from 24.2.x and 25.2.1xx have been forward ported to Release 25.2.107.

Release 25.2.106

Table 4-14 Alternate Route Service 25.2.106 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
38644699	TTL value in lookup is showing greater than the value defined in DNS SRV records in ARS	DNS SRV lookups processed by Alternate Route Service could have returned TTL values higher than those defined in the corresponding DNS SRV records, causing lookup responses to reflect an incorrect TTL.	2	25.2.106
35644465	ARS Metric oc_dns_srv_lookup_total does not peg as per the TTL	The `oc_dns_srv_lookup_total` metric could have incremented every 60 seconds regardless of the DNS SRV record TTL, resulting in lookup counts that did not reflect actual TTL-based lookup behavior.	3	23.2.3

> **Note**
>
> Resolved bugs from 24.2.x and 25.2.1xx have been forward ported to Release 25.2.106.

4.2.9.4 Common Configuration Service Resolved Bugs

Release 25.2.108

Table 4-15 Common Configuration Service 25.2.108 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
38828770	/nf-common-component/v1/igw/applicationparams API is returning multiple entries during Policy NF upgrade causing pod resrarts on audit service of PCF	During an in-service upgrade of PCF, the Gateway Services endpoint `/nf-common-component/v1/igw/applicationparams` returned multiple results, and the audit service could not determine which configuration to use and restarted.	2	25.2.106

> **Note**
>
> Resolved bugs from 25.2.1xx have been forward ported to Release 25.2.108.

4.2.9.5 NRF-Client Resolved Bugs

Release 25.2.102

Table 4-16 NRF-Client 25.2.102 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
38562170	Priority set to UNKNOWN for requests for AutonomousNfSubscriptionUpdate and AutonomousNfUnSubscribe (Nrf-Client 25.2.102)	After enabling Traffic Prioritization in the Egress Gateway Helm configuration, the default `trafficPrioritization` setting did not assign priority levels to `AutonomousNfUnSubscribe` and `AutonomousNfSubscriptionUpdate` messages, leaving them incorrectly marked as `UNKNOWN`.	2	25.2.200

Release 25.2.101

Table 4-17 NRF-Client 25.2.101 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
38450018	NRF-Client sending user-agent header while sending registration or hearbeat even when userAgentFlag set to false (25.2.101)	The NRF-Client was incorrectly sending the `User-Agent` header to the Egress Gateway microservice even when the `userAgent` flag was disabled.	2	25.2.100

Release 25.2.100

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 ATS Known Bugs

Release 25.2.202

There are no known bugs in this release.

4.3.2 BSF Known Bugs

Release 25.2.200

Table 4-18 BSF 25.2.200 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
39021617	500 Internal Error is received in the response code instead of 503 Method Not Allowed	When a request uses an unsupported method, the BSF Management service returns a 500 Internal Server Error instead of the expected Method Not Allowed error.	BSF Management service requests that use an unsupported HTTP method return HTTP 500 instead of HTTP 405 (Method Not Allowed). The response includes an internal error message about multiple exception handlers, which can mislead users and complicate error handling. **Workaround**: None	3	25.2.200

Table 4-18 (Cont.) BSF 25.2.200 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
38788026	Duplicate port definition warning is displayed while restarting BSF Management service and Query service	During fresh installation, upgrade, and restarts, BSF Management service and Query service display warnings about a duplicate container port definition for the monitoring and metrics port.	These warnings can cause install, upgrade, restart, or rollback operations to fail, which can impact service availability. During upgrade, Kubernetes can also remove the monitoring and metrics port, because the port is defined twice (one named and one unnamed), which can prevent metrics scraping. **Workaround**: None	3	25.2.200

4.3.3 CNC Console Known Bugs

Release 25.2.200

There are no new known bugs for this release.

4.3.4 cnDBTier Known Bugs

Release 25.2.201

Table 4-19 cnDBTier 25.2.201 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
38979458	SEPP-PERF-CNDB: ndbmysqld-3 stuck after rollback from 25.2.200-rc.7 to 25.2.101-GA	After upgrading the MySQL Cluster (OCC NDB tier) to a newer build and then performing a Helm rollback to the previously deployed stable build, one MySQL Server pod (ndbmysqld-3) fails to start and remains in CrashLoopBackOff. All other NDB components and the other MySQL Server pods continue running normally.	After a rollback, if this issue occurs, the ndbmysqld pod(s) may become stuck in the CrashLoopBackOff state. This happens because ndbmysqld can fail while attempting to create the local Data Dictionary (DD) from the NDB Data Dictionary. **Workaround**: A fatal GRR needs to perform to over come this issue.	2	25.2.200
38857144	Cluster Disconnect observed when horizontal scaling was performed for ndbappmysqld pods	Cluster gets disconnected during the scaling of the ndbappmysqld and ndbmysqld pods during the addition of Geo redundant site.	The cluster becomes disconnected when scaling ndbappmysqld and ndbmysqld pods during the process of adding a geo-redundant site. **Workaround**: The horizontal scaling of ndbappmysqld pods and the addition of cnDBTier geo-redundant sites procedures have been updated to address cluster disconnection issues during scaling operations.	2	25.2.100
38585013	dbtscale_vertical_pvc stuck for ndbapp pod in phase 4 with Waiting for localhost to restart on non-GR setup	The `dbtscale_vertical_pvc` service doesn't work on sites where replication to other sites has been configured, but only one site has been installed.	The dbtscale_vertical_pvc operation does not function correctly on sites configured for replication to additional sites when only a single site has been installed. **Workaround**: Perform the manual maintenance procedure for "Vertical Scaling - Updating PVC" for the affected StatefulSet or Deployment. For more information, see "Updating PVC Using Helm Upgrade" under "Vertical Scaling" section in *Oracle Communications Cloud Native Core, cnDBTier User Guide*.	2	25.2.100

Table 4-19 (Cont.) cnDBTier 25.2.201 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
38877149	Replication break observed with skip error enabled on site post ndbmysqld and ndbappmysqld pods complete scale down for 15 Min.	In previous releases, when the pods were scaled down and then scaled up, replication would come up successfully. However, in this release, replication is going down because the epoch loss exceeds the `epochTimeIntervalHigherThreshold` during that time window.	If the last applied epoch is missing from one of the standby ndbmysqld pods at the source site, and both replication ndbmysqld pods go down, replication resumes without verifying the skip-error logic that checks whether the ndbmysqld pods have been disconnected for longer than the configured threshold. Consequently, no skip-error information is recorded in this scenario. **Workaround**: Perform the georeplication recovery procedure if the replication is broken.	3	25.2.200
38921972	Replication delay 10hrs(36000sec secondsBehindRemote) during the CNCC upgrade.	An incorrect epoch value was used during skip error handling, which caused replication to restart from a previous point and reapply some transactions that had already been processed.	Replaying transactions that have already been applied results in temporary data inconsistencies between sites. **Workaround**: Before initiating the NF upgrade on any site, ensure that all db-replication-svc pods are restarted across every site.	3	24.2.6
38947690	100% Traffic failure on UDR when we restart one ndbmtd pod	Restarting a single ndbmtd (data node) pod results in unexpected cascading restarts across all ndbmtd pods, causing a full (100%) UDR traffic outage. During the initial ndbmtd pod restart, a cluster disconnect was also observed.	A cluster disconnect during ndbmtd pod restart activity can disrupt data node synchronization and may result in data inconsistencies across multiple sites. In addition, the cascading ndbmtd restarts can cause a complete UDR traffic outage. **Workaround**: During maintenance operations that may restart ndbmtd pods (for example, platform upgrades, cnDBTier upgrades, rollbacks, or scaling activities), reroute NF traffic to alternate cnDBTier clusters to avoid service impact.	3	25.2.200

4.3.5 CNE Known Bugs

Release 25.2.200

Table 4-20 CNE 25.2.200 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 platform agnostic bmCNE deployment procedure of X9-2 servers" from *Oracle Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide*. • Use CNE 24.3.1 or older version on X9-2 servers.	2	23.4.0

4.3.6 NSSF Known Bugs

Release 25.2.200

Table 4-21 NSSF 25.2.200 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
38819395	NSSF nsselection pod restarted with 143 Error Code During 80K TPS NS-Selection Traffic when the connection is recursively broken between mysql and ns-selection, ns-availability pods on site 1 for 10 minutes every 50 minutes	The issue occurs when DB connectivity to all pods is disrupted for 10 minutes and then restored for 50 minutes, repeating cyclically for over 12 hours. This pattern is highly unlikely in a real production setup. Additionally, the issue is intermittent, observed in only one environment and not reproducible in another setup.	Customer impact is low, as the scenario is rare and environment-specific. When a restart occurs, traffic resumes normally. During the restart window, only in-flight messages are affected, and only one out of eight NS-Selection pods is impacted, limiting overall service degradation. **Workaround:** None	3	25.2.200
38532145	CPU Utilization across ns-selection pods are not equally distributed.	CPU utilization variance (~10%) is observed between the highest and lowest utilized NS-Selection pods. Resource consumption is not evenly distributed across all pods.	There is no customer impact. Traffic handling remains stable with zero traffic loss and no service degradation observed. **Workaround:** None	3	25.2.200

Table 4-21 (Cont.) NSSF 25.2.200 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
38238999	oc_oauth_request_failed_cert_expiry Metric not getting pegged .	When an OAuth authentication is rejected because the certificate is expired, the message is correctly rejected as per validation logic. However, the corresponding metric is not being recorded, resulting in a monitoring gap.	Customer impact is low, as message validation and rejection behavior are functioning correctly. The issue is limited to observability, where the related metric is not being pegged. **Workaround:** None	3	25.2.200

Table 4-21 (Cont.) NSSF 25.2.200 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
38621015	If abatementValue is higher than onsetValue, NSSF should reject the overloadLevelThreshold configuration	Validation for the overload control API configuration is missing. This can allow incorrect parameter settings, potentially causing overload control to trigger (onset) without proper abatement.	There is potential service degradation risk if overload parameters are misconfigured, which may result in sustained overload control without recovery. However, the issue is configuration-related and avoidable with correct setup. **Workaround:** Configure overload control parameters as per the REST API guide, ensuring the abatement value is lower than the onset value to allow proper recovery behavior.	3	25.2.200

Table 4-21 (Cont.) NSSF 25.2.200 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
38621028	[72K TPS Success] [8K TPS Http Reset Stream] NSSF returns 503 for NS-Selection/ Availability Success Traffic (72K) - Success Rate Drops to 0.5% for ns-selection and 2.15% for ns-availability traffic	In a scenario where reset stream messages are sent for 10% of the traffic, an overall traffic loss of approximately 0.5% is observed.	There is a measurable impact of ~0.5% traffic loss when 10% of incoming traffic consists of reset streams. Outside this scenario, normal traffic handling remains unaffected. **Workaround:** None	3	25.2.200
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 intermittently accepts requests containing an invalid `Accept` header instead of rejecting them as expected.	There is no impact on traffic or service behavior. Traffic processing and success rate remain unaffected. **Workaround:** None	3	25.1.100
37784755	Option not available to change log level for pods "ocnssf-ocpm-config" & "ocnssf-performance" via CNCC and via REST	The *perf-info* microservice does not provide an option to modify the log level dynamically. It is currently fixed at the ERROR level.	There is no impact on customer traffic or call processing, as the *perf-info* microservice is not part of the live traffic handling or call flow path. Production services remain unaffected. **Workaround:** None	3	25.1.100

Table 4-21 (Cont.) NSSF 25.2.200 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 configured for keyId, certName, kSecretName, and certAlgorithm in the oauthValidator configuration are currently not being validated by the system. The configuration accepts incorrect or unsupported values without raising validation errors.	There is no impact on live traffic. However, the absence of validation may lead to misconfigurations remaining undetected until runtime verification or certificate usage scenarios occur. **Workaround:** Follow the REST API guide to configure certificate parameters. While configuring the oauthValidator, the operator must ensure that: • keyId matches the expected key identifier configured in the certificate. • certName corresponds to a valid and existing certificate reference. • kSecretName correctly maps to the intended	3	24.1.0

Table 4-21 (Cont.) NSSF 25.2.200 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
			Kubernetes secret. • certAlgorithm uses a supported and valid algorithm value.		

Table 4-21 (Cont.) NSSF 25.2.200 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
38843842	[27K TPS Each Site] Deleting All CNDB Pods in All 3 Sites Causes Irrecoverable Replication Breakage (Site 2 → Site 3) "The incident LOST_EVENTS occurred on the source. Message: cluster disconnect" Error, No Auto-Recovered	If all CNDB pods across the three GR sites are deleted simultaneously, the replication channel does not automatically re-establish after the pods restart. Manual intervention is required to restore replication.	• Loss of Group Replication (GR) connectivity between sites. • Potential for unexpected or inconsistent responses until replication is restored. • This represents a corner-case scenario, as it requires simultaneous deletion of all CNDB pods across all sites, which is rare and highly unlikely under normal operational conditions. **Workaround:** Run the GRR (Group Replication Recovery) procedure to manually restore replication connectivity	3	25.2.200

Table 4-21 (Cont.) NSSF 25.2.200 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
			between the sites.		
38819080	NSSF ns-selection Istio-Proxy pod crashed During 80K TPS NS-Selection traffic When All NSSF Pods Are Deleted on Site 1	When all pods are deleted using "kubectl delete pod --all -n ", one of the sidecar ASM (Aspen Service Mesh) Istio containers crashed.	This behavior is observed only in a corner-case scenario where all pods are forcefully deleted simultaneously, which is not representative of normal production or rolling upgrade operations. The ASM sidecar crash occurs during pod termination, after the pod has already been removed from active service endpoints. As a result, there is no significant impact to customer traffic or service availability. As this happens when all pods are deleted, there is minimal loss because of this crash. **Workaround:** None	3	25.2.200

Table 4-21 (Cont.) NSSF 25.2.200 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
38552515	GW Metrics issues for NSSF 54K Success Scenario and 26K failure [Slice is not configured in PlmnInfo] TPS traffic on single site.	A mismatch is observed in `oc_ingressgateway_http_responses_total` metrics.503 responses are not consistently pegged.Back end 403 (SNSSAI_NOT_SUPPORTED) is recorded as 500 or `error_reason="UNKNOWN"` .IGW metrics do not accurately reflect actual backend response codes.	There is no impact on traffic or service behavior; backend responses remain correct (403 for invalid slice cases). The impact is limited to observability, as metrics do not accurately reflect actual response codes. 403 errors may appear as 500, and 503 responses may not be consistently pegged, leading to inaccurate monitoring visibility. **Workaround:** None	3	25.2.200
38796537	Encountered 500 error response in NS-Availability call flow during an 80K TPS load at Site 1	In a long run of more than 100 hours, intermittently in some setups, 0.003% of messages are failing with 5xx responses. This is happening in a specific setup; in other setups, this is not observed.	Intermittently, 0.003% message loss. **Workaround:** None	3	25.2.200

Table 4-21 (Cont.) NSSF 25.2.200 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
38901019	NS-selection pods are being deleted one by one at 5-minute intervals, One of the NS-selection pods is utilizing only 1% of CPU after comes up ns-selection pods, success rate dropped 0.003% traffic.	NS-selection pods were deleted sequentially at 5-minute intervals. After restart, one of the pods was utilizing only ~1% CPU. During this period, the overall success rate dropped by 0.003% of traffic.	The impact was negligible, with only a very small (0.003%) reduction in success rate. There was no significant service degradation or large-scale traffic loss observed. **Workaround:** None	3	25.2.200
39008266	NSSF should reject avail put and patch request if SST type is string.	NSSF is expected to reject PUT and PATCH requests when the SST parameter is provided in an incorrect format (e.g., string type). Currently, NSSF accepts requests where the SST parameter is sent with an empty string ("") instead of a valid integer value.	• Impact occurs only when a peer NF sends an invalid SST value (empty string instead of integer). • No impact on live traffic handling or normal service behavior. • Valid requests with correctly formatted SST values continue to function as expected. **Workaround:** None	3	25.2.200

Table 4-21 (Cont.) NSSF 25.2.200 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
38628736	While doing the scale down to 0 all NSSF deployment, NSSF Pods Enter Error State Before Termination During Scale-Down to 0.	During scale-down of all NSSF deployments to zero replicas, several pods briefly enter the Error state before complete termination. Instead of terminating gracefully, pods transition through an Error status during the shutdown process.	There is no impact on live traffic, as this scenario occurs during an intentional scale-down to zero. The issue is limited to pod lifecycle behavior during shutdown and does not affect service functionality when the system is operational. **Workaround:** None	4	25.2.200
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 string is not in line with expectations when the Kid does not match. Instead of responding with “Kid does not match,” the response string contains “kid missing.”	Minimal impact, as the error code is correct; only the description string is incorrect. **Workaround:** None	4	24.1.0
38941167	[25.2.200]: Dynamic Logging Feature: With commonCfgClient. enabled set to false run time log level of services is still getting updated	When commonCfgClient.enabled is set to false, the log level update during runtime must not be allowed, but it is being allowed.	No impact on traffic. Runtime log level update is enabled by default. Until the log level change with op gui is triggered, the log level does not change. **Workaround:** None	4	25.2.200

Table 4-21 (Cont.) NSSF 25.2.200 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
38973933	Encountered 500 and 404 error response in NS-Availability Call Flow after site restore	In a 3-site GR deployment handling ~27K TPS per site, failover was triggered sequentially for Site 3 and Site 2, resulting in traffic being redirected to Site 1 as the single active site. During this period, replication channels for the failed sites were temporarily broken. Once Site 2 and Site 3 were restored, traffic was redistributed and replication channels were successfully re-established across all sites. During the dual-site outage scenario (traffic converging to one active site), approximately 0.003% of messages were lost.	A very minimal traffic impact was observed, with 0.003% message loss during the scenario where two sites were down and all traffic was handled by a single active site. No prolonged service outage occurred, and full replication and traffic distribution were restored after site recovery. **Workaround:** None	4	25.2.200

Table 4-21 (Cont.) NSSF 25.2.200 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
39015332	LCI header contains NfInstance ID but does not contain serviceInstanceId	The LCI header includes the NfInstanceId, but the serviceInstanceId is not present in the header.	• No impact on traffic handling or service functionality. • Absence of the serviceInstanceId in the LCI header may reduce service-level traceability and granular monitoring at the instance level. • ServiceInstanceId provides service-level information; however, this information can be clearly inferred from the API URI, thereby minimizing functional impact. **Workaround:** None	4	25.2.200

4.3.7 OCCM Known Bugs

Release 25.2.200

There are no known bugs in this release.

4.3.8 OSO Known Bugs

Release 25.2.200

There are no known bugs in this release.

4.3.9 Common Services Known Bugs

4.3.9.1 Alternate Route Service Known Bugs

Release 25.2.2xx

There are no known bugs in this release.

4.3.9.2 Egress Gateway Known Bugs

Release 25.2.2xx

Table 4-22 Egress Gateway 25.2.2xx Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
39049678	Improve logging when catching NPE during Jetty Bean creation when TLS disabled deployment	The following error log is observed, showing a NullPointerException (NPE) during web bean creation in REST mode installation: `{"instant": {"epochSecond":1772635550,"nanoOfSecond":783737564},"thread":"pool-13-thread-1","level":"ERROR", "loggerName":"ocpm.cne.gateway.util.WebClientRoutingFilterBeanManager", "message":"Cannot invoke \"ocpm.cne.gateway.ssl.extension.ReloadableX509KeyManager.getDefaultKeyManager()\" because \"this.reloadableX509KeyManager\" is null", "endOfBatch":false,"loggerFqcn":"org.apache.logging.log4j.spi.AbstractLogger","threadId":82,"threadPriority":5, "messageTimestamp":"2026-03-04T14:45:50.783+0000","ocLogId":"","xRequestId":"","pod":"","processId":"1","instanceType":`	It might have Observability impacted due to an unexpected error log during installation. **Workaround**: None	3	25.2.108

Table 4-22 (Cont.) Egress Gateway 25.2.2xx Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
		"prod","egressTxId":""} at org.springframework.context.event.SimpleApplicationEventMulticaster.doInvokeListener(SimpleApplicationEventMulticaster.java:163) at org.springframework.context.event.SimpleApplicationEventMulticaster.invokeListener(SimpleApplicationEventMulticaster.java:156) at org.springframework.context.event.SimpleApplicationEventMulticaster.multicastEvent(SimpleApplicationEventMulticaster.java:134) at org.springframework.context.support.AbstractApplicationContext.publishEvent(AbstractApplicationContext.java:434) at org.springframework.context.support.AbstractApplicationContext.publishEvent(AbstractApplicationContext.java:367) at com.oracle.common.scheduler.Reload			

Table 4-22 (Cont.) Egress Gateway 25.2.2xx Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
		Config.reloadProperties(ReloadConfig.java:217) at java.base/jdk.internal.reflect.NativeMethodAccessorImpl.invoke0(Native Method) at java.base/jdk.internal.reflect.NativeMethodAccessorImpl.invoke(NativeMethodAccessorImpl.java:77) at java.base/jdk.internal.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:43) at java.base/java.lang.reflect.Method.invoke(Method.java:568) at org.springframework.scheduling.support.ScheduledMethodRunnable.run(ScheduledMethodRunnable.java:73) at org.springframework.scheduling.support.DelegatingErrorHandlingRunnable.run(DelegatingErrorHandlingRunnable.java:43) at java.base/java.util.concurr			

Table 4-22 (Cont.) Egress Gateway 25.2.2xx Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
		ent.Executors$RunnableAdapter.call(Executors.java:539) at java.base/java.util.concurrent.FutureTask.runAndReset(FutureTask.java:305) at java.base/java.util.concurrent.ScheduledThreadPoolExecutor$ScheduledFutureTask.run(ScheduledThreadPoolExecutor.java:305) at java.base/java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1136) at java.base/java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:635) at java.base/java.lang.Thread.run(Thread.java:842)			

Table 4-22 (Cont.) Egress Gateway 25.2.2xx Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
39083890	EGW logs for message "HTTP response body is empty" doesn't contains ocLogId	When an error response is received from a peer NF, PCF EGW generates logs that do not include ocLogId, causing those logs to be missed when filtering by ocLogId. Log Snippet/Metrics used: `{"instant":{"epochSecond":1773547547,"nanoOfSecond":325432825},"thread":"egw-app-thread9","level":"WARN","loggerName":"ocpm.cne.gateway.pcf.filters.SubActLogGatewayFilterFactory","message":"HTTP response body is empty.","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger","threadId":142,"threadPriority":5,"messageTimestamp":"2026-03-15T04:05:47.325+0000","ocLogId":"","xRequestId":"","pod":"ocpcf-occnp-egress-gateway-6c96788594-xdw8p","processId":"1","instanceType":"prod","egressTxId":"egress-tx-1984554961"}`	Debugging is impacted because not all logs include ocLogId. **Workaround**: None	3	25.2.108

Table 4-22 (Cont.) Egress Gateway 25.2.2xx Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
39123626	occnp_oc_egressgateway_outgoing_ip_type is missing dimension DestinationHost	With PCF 25.2.200-LA and GW 25.2.109.0.0, the occnp_oc_egressgateway_outgoing_ip_type metric is missing the DestinationHost dimension, although it was present in the PCF 25.2.200 test release and GW 25.2.108.0.0.	Impact on observability in error scenarios and on system performance. **Workaround**: None	3	25.2.109
39088228	Host dimension in Egress gateway response metrics still has cardinality explosion	In the Egress Gateway 25.2.109 test release, the Host dimension parameter is supported as part of Egress Gateway cardinality for Egress Gateway response metrics.	Impacts observability in error scenarios and affects system performance. **Workaround**: None	3	25.2.109
37751607	Egress gateway throwing NPE when trying to send oauth token request to "Default NRF Instance" when unable to find NRF instance to forward the request	Egress Gateway failed to send requests to the configured primaryNrfApiRoot and secondaryNrfApiRoot endpoints specified in the configmap. Subsequently, it attempted to send an OAuth2 token request to the default NRF instance at "[http://localhost:port/oauth2/token]," but this request also failed. Egress Gateway displayed a NullPointerException.	This issue occurs only when an invalid host and port are provided. The port is mentioned with string value as "port" instead of a numeric port value, for example, 8080. **Workaround**: You must provide the valid host and port for the NRF client instance.	3	25.1.200

Table 4-22 (Cont.) Egress Gateway 25.2.2xx Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
38339561	Metrics oc_ingressgateway_dd_unreachable and oc_egressgateway_dd_unreachable are not resetting to value zero after connection with DD is restored	After the connection with Oracle Communications Network Analytics Data Director is restored, the oc_ingressgateway_dd_unreachable and oc_egressgateway_dd_unreachable metrics do not reset to 0.	It has observability impact as even the connection is restored, the metric is not updated. **Workaround**: None	3	24.1.5
38504941	EGW/IGW should include LCI header when the current load is less than or equals to the difference between previously reported load and configured LoadThreshold value	Ingress Gateway and Egress Gateway do not include the LCI header when the current load is less than or equal to the difference between the previously reported load and the configured LoadThreshold.	It has an impact on consumer NF to decide for traffic load as LCI information is not shared when the current load is less than or equal to the difference between the previously reported load and the configured LoadThreshold. **Workaround**: None	3	25.2.102
38304085	EGW is not Validating 3gpp-sbi-message-priority Header parameters in case of POP25 and Overload	Egress Gateway do not validate the 3gpp-sbi-message-priority header parameters in the pod protection overload scenarios.	This Config validation issue causes the feature to malfunction in case invalid values are received. **Workaround**: The consumer NF should send valid values in the header to avoid any malfunctioning.	3	25.2.100

Table 4-22 (Cont.) Egress Gateway 25.2.2xx Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
38294514	Observed NPE during oauth-acess-request message when "nrfClientQueryEnabled" flag enabled	An NPE is observed during the oauth-access-request message when the nrfClientQueryEnabled parameter is enabled.	Due to Null Pointer Exception (NPE), the OAuth access token request does not reach the NRF, and more calls fail because the OAuth token request is failing. **Workaround**: None	3	25.2.100
38279961	"oauthDeltaExpiryTime" functionality not working during traffic run. Somtimes EGW is requesting NRF oauthtoken even though still ""oauthDeltaExpiryTime" not expired.	The oauthDeltaExpiryTime functionality does not work during traffic run. Egress Gateway requests an NRF OAuth token before the configured oauthDeltaExpiryTime expires.	There is no traffic impact because token request processing occurs before timerExpiry. **Workaround**: None	3	25.2.100
38778598	occnp_oc_egressgateway_outgoing_ip_type metric updated for IPv4 in IPv6 preferred dual stack deployment even DNS removed IPv4 address from DNS response for NRF	In an IPv6 preferred dual stack deployment, the `occnp_oc_egressgateway_outgoing_ip_type` metric is updated for IPv4 even when DNS removes the IPv4 address from the DNS response.	Incorrect information about active connections is provided when DNS records change from IPv4 to IPv6 or vice versa, even when the old connections have already terminated. **Workaround**: None	3	25.2.104

Table 4-22 (Cont.) Egress Gateway 25.2.2xx Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
38810446	Missing ignoremaxresponsertime & sbiRoutingWeightBasedEnabled under metadata in EGW CNCC screen	In the Egress Gateway CNC Console screen, the `ignoremaxresponsertime` and `sbiRoutingWeightBasedEnabled` metadata fields are missing, so these fields cannot be included when the route is configured or edited. This affects SBITimer and NRF route automation functionality over Egress Gateway and may prevent the feature from working.	• Load sharing is not supported among Producer NFs because the default setting for `sbiRoutingWeightBasedEnabled` is false. • The SBI Timer feature cannot be used for plmn-egw unless `IgnoreMaxRspTimeHeader` is explicitly set to false in the route configuration. **Workaround**: Configure the routes using REST APIs instead of using the CNC Console.	3	25.2.106

Table 4-22 (Cont.) Egress Gateway 25.2.2xx Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
38810483	No support for header based predicate under EGW Routesconfig uration in CNCC screen	The CNC Console screen does not support a header-based predicate in Egress Gateway route configuration, so routes cannot be configured that use a header name as a filter.	The NRF route configuration is affected because it relies on a header-based predicate at plmn-egw. This may impact inter-PLMN NRF requests that pass through SEPP. **Workaround**: None	3	25.2.106

4.3.9.3 Ingress Gateway Known Bugs

Release 25.2.2xx

Table 4-23 Ingress Gateway 25.2.2xx 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 the controlledshutdown errormapping and errorcodeprofiles are not present. This indicates that the required action of rejecting traffic will not occur. There must be a pre-check to check for these configurations before allowing the state to be changed. If the pre-check fails, the operational state should not be changed.	Request will be processed by Gateway Services when it is supposed to be rejected. **Workaround**: None	3	23.2.0

Table 4-23 (Cont.) Ingress Gateway 25.2.2xx Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
38339561	Metrics oc_ingressgateway_dd_unreachable and oc_egressgateway_dd_unreachable are not resetting to value zero after connection with DD is restored	After the connection with Oracle Communications Network Analytics Data Director is restored, the oc_ingressgateway_dd_unreachable and oc_egressgateway_dd_unreachable metrics do not reset to 0.	It has observability impact as even the connection is restored, the metric is not updated. **Workaround**: None	3	24.1.5
38405814	Post_rollback_SM_ Validation fails at alternate-route logging level validation	The alternate-route logging level values are mismatching.	It has no impact because it is not a production use case. The log level is not changed from WARN to DEBUG. **Workaround**: None	3	25.2.100
38310333	In TLS setup when IGW rejected with 401 then IGW Request/Response Latency metrics are not updated	In a TLS setup, when Ingress Gateway rejects a request with HTTP 401, the Ingress Gateway request and response latency metrics are not updated.	It has observability impact because the latency metric is not being updated. **Workaround**: None	3	25.2.100
38293511	IGW is not Validating 3gpp-sbi-message-priority Header parameters in case of POP25 and Overload	Ingress Gateway does not validate the 3gpp-sbi-message-priority header parameters in the pod protection overload scenarios.	This Config validation issue causes the feature to malfunction in case invalid values are received. **Workaround**: The consumer NF should send valid values in the header to avoid any malfunctioning.	3	25.2.100

Table 4-23 (Cont.) Ingress Gateway 25.2.2xx Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
38181400	NPE seen in one of the IGW pod during pod initialization	In Ingress Gateway 25.1.203, an NPE occurs in one of the Ingress Gateway pods during initialization in an idle state when no traffic is sent.	Due to Null Pointer Exception (NPE), the OAuth access token request does not reach the NRF, and more calls fail because the OAuth token request is failing. **Workaround**: None	4	25.1.203
37986338	For XFCC header failure case "oc_ingressgateway_http_responses_total" stats are not updated	When deploying Ingress Gateway with XFCC header validation enabled in a three-route configuration (for create, delete, and update operations), and sending traffic without the XFCC header, Ingress Gateway rejected the traffic due to XFCC header validation failure. However, the `oc_ingressgateway_http_responses_total` metric was not updated, but the `oc_ingressgateway_xfcc_header_validate_total` metric was updated.	The metric will not be pegged when the XFCC header validation failure is observed. **Workaround**: None	4	25.1.200
38461465	Sender Attribute should only consist SEPP-<sepp-fqdn> when addtional error logging in enabled in gw logging config	When any failure is observed in Gateway Services, the sender attribute format does not aligned with SEPP requirements when additional error logging is enabled in the Gateway Services logging configuration.	It has observability and debugging impact because it is a formatting issue for SEPP and SCP. **Workaround**: None	4	25.2.100

Table 4-23 (Cont.) Ingress Gateway 25.2.2xx Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
38769987	oc_ingressgateway_sbitimer_timezone_mismatch gauge metrics once pegged does not reset	The `oc_ingressgateway_sbitimer_timezone_mismatch` metric does not reset to 0 after it is configured, and it remains 1 even after reset is attempted.	Observability impact will be there because metric is not getting reset. **Workaround**: None	3	25.2.105
38771574	SBITimer Feature Enabled-sbiTimerTimezone related Issues	When the Gateway Services time zone is set to `ANY`, requests that include a PDT time zone are processed in GMT because the current time and sender time are converted to GMT. When `ANY` is set and the request has no time zone, a late arrival error occurs even though the time zone cannot be identified.	When the configured time zone is `ANY` and a time zone is not included in the header, an incorrect late arrival error is received instead of a wrong format error. When the configured time zone is `GMT` and a different time zone is sent, the timestamp interpretation can cause an incorrect late arrival error if the effective times do not match. **Workaround**: Ensure that the configuration and the timestamp in the header align with the configured time zone.	3	25.2.105
38817374	IGW reported NPE during installation when config server is unreachable	Ingress Gateway reports NPE during installation when config server is unreachable.	Incorrect information is received about connectivity issues between Gateway Services and the config server when the config server is not yet fully up. **Workaround**: None	3	25.2.106

4.3.9.4 Common Configuration Service Known Bugs

Release 25.2.2xx

There are no known bugs in this release.