Oracle® Communications

Cloud Native Core Release Notes

Release 3.25.1.200.0
G36884-09
September 2025

Oracle Communications Cloud Native Core Release Notes, Release 3.25.1.200.0

G36884-09

Contents

Preface

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 customer access to and use of Oracle support services will be pursuant to the terms and conditions specified in their Oracle order for the applicable services.

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 you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you 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 3.25.1.200 - G36884-09, September 2025

cnDBTier 25.1.201 Release

- Updated the section cnDBTier Resolved Bugs with the details of cnDBTier release 25.1.201.
- Updated the section cnDBTier Known Bugs with the details of cnDBTier release 25.1.200.

SCP 25.1.201 Release

Updated the following sections with the details of SCP release 25.1.201:

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

Release 3.25.1.200 - G36884-08, August 2025

Updated the following sections with the details of cnDBTier release 25.1.201:

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

Release 3.25.1.200.0 - G36884-06, August 2025

Updated the Policy section for Policy 25.1.200.

Release 3.25.1.200.0 - G36884-05, August 2025

NRF 25.1.200 Release

Updated the NRF Resolved Bugs section with a new bug (35672666) details.

SEPP 25.1.201 Release

Updated the following sections with the details of SEPP release 25.1.201:

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

Release 3.25.1.200.0 - G36884-04, July 2025

Updated the Compatibility Matrix section for Policy 25.1.200.

Release 3.25.1.200.0 - G36884-03, July 2025

SEPP ATS 25.1.201 Release

Updated the following sections with the details of SEPP ATS release 25.1.201:

- SEPP Resolved Bugs
- Media Pack

CNE 25.1.200 Release

Updated the CNE Resolved Bugs section for CNE 25.1.200.

cnDBTier 25.1.200 Release

Updated the cnDBTier Resolved Bugs section for cnDBTier 25.1.200.

Release 3.25.1.200.0 - G36884-02, July 2025

SCP 25.1.200 Release

Updated the following sections with the details of SCP release 25.1.200:

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

Release 3.25.1.200.0 - G36884-01, July 2025

General Updates:

Updated the Generic Open Source Software Compatibility on Any Platform section to provide information about the open source software compatibility with CNC NFs for 3.25.1.2xx.0 release.

BSF 25.1.200 Release

Updated the following sections with the details of BSF release 25.1.200:

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

- BSF Resolved Bugs
- BSF Known Bugs

cnDBTier 25.1.200 Release

Updated the following sections with the details of cnDBTier release 25.1.200:

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

CNC Console 25.1.200 Release

Updated the following sections with the details of CNC Console release 25.1.200:

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

CNE 25.1.200 Release

Updated the following sections with the details of CNE release 25.1.200:

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

NRF 25.1.200 Release

Updated the following sections with the details of NRF release 25.1.200:

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

NSSF 25.1.200 Release

Updated the following sections with the details of NSSF release 25.1.200:

- 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 25.1.200 Release

Updated the following sections with the details of OCCM release 25.1.200:

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

OCI Adaptor 25.1.200 Release

Updated the following sections with the details of OCI Adaptor release 25.1.200:

- OCI Adaptor
- Compatibility Matrix

Policy 25.1.200 Release

Updated the following sections with the details of Policy release 25.1.200:

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

SEPP 25.1.200 Release

Updated the following sections with the details of SEPP release 25.1.200:

- Security Edge Protection Proxy (SEPP)
- Media Pack
- Compatibility Matrix

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

UDR 25.1.200 Release

Updated the following sections with the details of UDR release 25.1.200:

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

Common Services Resolved Bugs

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

Common Services Known Bugs

- Egress Gateway Known Bugs
- Ingress Gateway Known Bugs

1

Introduction

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

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

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

2
Feature Descriptions

This chapter provides a summary of new features and updates to the existing features for network functions released in Cloud Native Core release 3.25.1.2xx.0.

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

2.1 Automated Testing Suite (ATS) Framework

Release 25.1.200

Oracle Communications Cloud Native Core, Automated Testing Suite (ATS) Framework 25.1.200 includes the following enhancements:

- **ATS Helm Enhancements**: This enhancement automates preinstallation and postinstallation steps of ATS deployment by eliminating the manual method.
- **Trace Validation Enhancements:** The trace validation framework has been enhanced to incorporate configurable retry mechanisms, support duration validation for checking the execution time of microservices, and apply filters to any microservice within a sequence.

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 CSloud Native Core, Automated Test Tools and Scripts Suite - Node Perpetual	CCNC-9803	ATS Helm Enhancements
Oracle Communications Cloud Native Core, Automated Test Tools and Scripts Suite - Node Perpetual	CCNC-9801	Trace Validation Enhancements

2.2 Binding Support Function (BSF)

Release 25.1.200

Oracle Communications Cloud Native Core, Binding Support Function (BSF) 25.1.200 includes the following enhancements:

- **Stale Binding Deletion Logging Enhancement**: BSF logs have been enhanced for stale session detection and removal by the audit service. You can now configure logs to be generated at either WARN or INFO level. For more information, see the "Enhanced

Logging of BSF Stale Binding Deletion" section in *Oracle Communications Cloud Native Core, Binding Support Function User Guide.*

- **Support for ASM 1.21.6:** BSF 25.1.200 supports Aspen Service Mesh (ASM) 1.21.6 version on Kubernetes 1.27 version from this release. For more information, see the "Configuring BSF to Support Aspen Service Mesh" section in *Oracle Communications Cloud Native Core, Binding Support Function Installation, Upgrade, and Fault Recovery Guide*.
- **Support for four site Georedundancy**: BSF supports four site georedundancy. For more information about this feature, see the "Georedundance Support" section in *Oracle Communications Cloud Native Core, Binding Support Function User Guide.*
- **Support for Dual Stack**: Using the dual stack mechanism, BSF communicates within services or deployments in a Kubernetes cluster using IPv4 or IPv6 or both simultaneously depending on the configured deployment mode. For more information about this feature, see the "Support for Dual Stack" section in *Oracle Communications Cloud Native Core, Binding Support Function User Guide.*
- **Pod Congestion Control for BSF Management Service**: The BSF Management service uses Pod Congestion Control to manage heavy incoming request traffic. It evaluates each request, accepting or rejecting it based on request priority and current congestion levels. For more information, see the "Pod Congestion Control for BSF Management Service" section in *Oracle Communications Cloud Native Core, Binding Support Function User Guide.*
- **Diameter Gateway Pod Congestion Control**: The Diameter Gateway Pod Congestion Control feature is modified to work with common Congestion Control mechanism. The user needs to migrate data from the older configuration parameters to the current Congestion Control feature. For more information about the data migration, see the "Diameter Pod Congestion Control "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 2-2 License names for feature mapping

License Name	CCNC Number	Feature Name
Oracle Communications Cloud Native Core, Binding Support Function - 25K Active Subscribers Perpetual	CCNC-8862	Stale Binding Deletion Logging Enhancement
Oracle Communications Cloud Native Core, Binding Support Function - 25K Active Subscribers Perpetual	CCNC-9617	Support for ASM 1.21.6
Oracle Communications Cloud Native Core, Binding Support Function - 25K Active Subscribers Perpetual	CCNC-3925	Support for four site Georedundancy
Oracle Communications Cloud Native Core, Advance Networking - 25K Active Subscribers	CCNC-10085	Support for Dual Stack

2.3 Cloud Native Environment (CNE)

Release 25.1.200

Oracle Communications Cloud Native Core, Cloud Native Environment (CNE) 25.1.200 includes the following enhancements:

- **Support for Sensitive data storage**: When installing or upgrading Cloud Native Environment (CNE), you must provide a `secrets.ini` file containing values for variables classified as sensitive.
  For more information, see the following sections in *Oracle Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide*:
  - Deploying CNE Cluster in OpenStack Environment
  - Predeployment Configuration for VMware
  - Configuring `secrets.ini` and `occne.ini` files
  - Environmental Variables
- **Customizing GRUB password**: GRUB password can be customized to do maintenance tasks on the boot process for every host of a cluster. Add or modify the `occne_grub_password` variable in the `hosts.ini` or `occne.ini` file according to your cluster. This is a mandatory parameter required to be configured during install or upgrade. Set the value of the `occne_grub_password` variable to the required password. Before setting a password, ensure that the password you choose comply to the following conditions:
  - Contain at least eight characters.
  - Contain uppercase and lowercase characters.
  - Contain at least special character except single and double quotes, ", ', \, %, &, and $.
  - Contain at least two digits.

  For more information, see the "Configuring GRUB Password" 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 - 3.17.1
  - Kubernetes - 1.32.0
  - containerd - 1.7.24
  - Calico - 3.29.1
  - MetalLB - 0.14.4
  - Prometheus - 3.2.0
  - Grafana - 9.5.3
  - Jaeger - 1.65.0
  - Istio - 1.18.2
  - Kyverno - 1.13.4
  - cert-manager - 1.12.4

To get the complete list of third-party services and their versions, refer to the `dependencies_25.1.200.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.

Operations Services Overlay (OSO)

Release 25.1.200

Oracle Communications Cloud Native Core, Operations Services Overlay (OSO) 25.1.200 includes the following enhancement:

- **Alert Automation**: With this feature, OSO supports other NFs to install and update alert configurations using the Helm chart. For more information about the feature, see the "Alert Automation" section in *Oracle Communications Cloud Native Core, Operations Services Overlay User Guide*.
  For detailed instructions on configuring this feature, see the "Automated Configuration of NF Alerts" section in *Oracle Communications Cloud Native Core, Operations Services Overlay Installation and Upgrade 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 2-3 License names for feature mapping

License Name	CCNC Number	Feature Name
Oracle Communications Cloud Native Core, Cloud Native Environment - per 25K Subscribers Perpetual	CCNC-9086	Alert Automation

2.4 Cloud Native Core cnDBTier

Release 25.1.201

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

Release 25.1.200

Oracle Communications Cloud Native Core, cnDBTier (cnDBTier) 25.1.200 includes the following enhancements:

- **Support for cnDBTier Backup Status APIs in CNC Console**: With this enhancement, cnDBTier NDB Backup status can be viewed on CNCC Console GUI. NF applications can check if the NDB cluster is performing a backup. This helps to prevent NF schema changes that may cause upgrade failures using the new screen. Additionally, a new API is added for this enhancement.

  For more information on the Backup Status API, see the "cnDBTier APIs" section in *Oracle Communications Cloud Native Core, cnDBTier User Guide*.
- **cnDBTier Metrics reorganization**: In the earlier implementation, metrics collection followed a centralized model where all metrics were gathered solely through the monitoring

service. While functional, this approach led to performance bottlenecks. The monitoring service became heavily loaded, resulting in slow metrics retrieval and, at times, resource spillage in terms of CPU and memory consumption. To address these issues, the metrics collection process has been distributed. Wherever feasible, metrics are now offloaded to the respective microservices. This decentralization reduces the load on the central monitor service, significantly improving the efficiency and speed of metrics retrieval.

As part of this new design, the infrastructure monitor component has been embedded as a permanent container within each relevant microservice. While this increases the overall resource footprint, it ensures a more scalable, responsive, and resilient monitoring framework.

> **Note**
>
> With multiple distributed endpoints now serving metrics, Prometheus must be appropriately scaled/resourced to handle the increased load and maintain scraping efficiency.

For more information on cnDBTier Metrics, see the "Metrics" section in *Oracle Communications Cloud Native Core, cnDBTier User Guide.*

- **Support for ASM 1.21.6**: cnDBTier 25.1.200 supports Aspen Service Mesh (ASM) 1.21.6 version on Kubernetes 1.27 version from this release.
- **Support for HTTPS communication**: The initial HTTPS implementation in cnDBTier lacked support for transitioning between HTTPS-disabled and HTTPS-enabled states. It also did not provide HTTPS functionality for CNLB. These limitations resulted in incomplete HTTPS support across different deployment scenarios. The current implementation addresses these limitations by providing comprehensive HTTPS support throughout cnDBTier. Enhancements include:
  - Seamless transition between HTTPS enabled and disabled states
  - Robust handling of HTTPS across all relevant components, including CNLB
  - Consistent and reliable secure communication in all configurations

  This update guarantees end-to-end HTTPS functionality, improving security and system consistency in various deployment scenarios. For more information about this feature enhancement, see *Oracle Communications Cloud Native Core, cnDBTier User Guide and Oracle Communications Cloud Native*.
- **Support for Dual Stack**: cnDBTier supports deployment on dual stack Kubernetes infrastructure, enabling communication over both IPv4 and IPv6. Using the dual stack mechanism, cnDBTier can establish and accept connections within pods and services using either IP family and interact seamlessly with external systems that support IPv4 and IPv6. In this setup, cnDBTier can use IPv4 or IPv6 for internal communication between its microservices, while external communication can be independently configured to use IP family. Additionally, the preferred IP family can be changed dynamically after deployment, providing enhanced flexibility in managing network configurations. For more information about this feature enhancement, see *Oracle Communications Cloud Native Core, cnDBTier User Guide* and *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*.
- **cnDBTier Helm (MOP) Enhancements**: Starting with version 25.1.200, cnDBTier supports the automated creation of service accounts, roles, and role bindings. While this functionality was available in older versions, the latest release introduces validation for manually created service accounts. Helm charts now verify whether a manually created service account has the required permissions.

The configuration has also been restructured to support different service accounts, including:

- Upgrade service account
- Application service account
- Multus service account

For detailed configuration instructions, see *Oracle Communications Cloud Native Core, cnDBTier 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 2-4 License names for feature mapping

License Name	CCNC Number	Feature Name
Oracle Communications Cloud Native Core, Policy Control Function - 25K Active Subscribers Perpetual	CCNC-9368	Support for ASM 1.21.6
Oracle Communications Cloud Native Core, Automated Lifecycle Management - 25K Active Subscribers	CCNC-9100	cnDBTier Helm (MOP) Enhancements
Oracle Communications Cloud Native Core, Advance Networking - 25K Active Subscribers	CCNC-8894	Support for Dual Stack

2.5 Cloud Native Configuration Console (CNC Console)

Release 25.1.200

Oracle Communications Cloud Native Configuration Console (CNC Console) 25.1.200 includes the following enhancements:

- **Lifecycle Management (LCM) Automation**: Lifecycle Management (LCM) Automation optimizes the deployment and upgrade processes for CNC Console by reducing the steps required to initiate. The following automation enhancements are supported in this release:
  - Helm Enhancements for Service Account: An automated resource creation has been introduced to streamline Kubernetes resource management through Helm charts.
  - Helm Enhancements for NF Alert Configurations on OSO: CNC Console leverages the `oso-alr-config` Helm chart, introduced in the OSO package, to apply alert rules through Helm upgrades. While the `oso-alr-config` Helm chart is deployed automatically during the OSO installation, the CNC Console performs Helm upgrades to apply or update the required alert rules. Both manual and automated configurations are supported.

  For more information, see *Oracle Communications Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide* and *Oracle Communications Cloud Native Configuration Console User Guide*.
- **Support for ASM 1.21.6**: CNC Console now supports Aspen Service Mesh (ASM) version 1.21.6. For more information, see *Oracle Communications Cloud Native Configuration Console 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, Automated Lifecycle Management - 25K Active Subscribers	CCNC-9092	Lifecycle Management (LCM) Automation
Oracle Communications Cloud Native Core, Advanced Cloud Native Environment – 25K Active Subscribers Perpetual	CNCC-8616	Support for ASM 1.21.6

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

Release 25.1.200

Oracle Communications Cloud Native Core, Certificate Management (OCCM) 25.1.200 includes the following enhancement:

- **Updating Certificate Configurations:** This feature enables updating essential fields in the certificate configuration. Based on changes to the end-entity certificate configuration, OCCM automatically recreates the certificate or applies updates during future renewals. 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	CNCC-8148	Updating Certificate Configurations

2.7 Network Repository Function (NRF)

Release 25.1.200

Oracle Communications Cloud Native Core, Network Repository Function (NRF) 25.1.200 includes the following enhancements:

- **Ingress Gateway Pod Protection Using Rate Limiting**: This feature applies a rate limiting mechanism to Ingress Gateway pods, allowing them to process a predefined number of requests. When the request rate exceeds the configured threshold, the pods protect themselves by either rejecting additional requests with a custom error code or allowing them, based on the configuration.

For more information about this feature, see the "Ingress Gateway Pod Protection Using Rate Limiting" section in *Oracle Communications Cloud Native Core, Network Repository Function User Guide*.

- **Writing Messages of the Same Transaction in the Same Kafka Partition:** This feature ensures that NRF copies request and response messages of the same transaction to the same Kafka partition when sending messages to Data Director. This reduces latency in processing transaction data. The feature uses the *correlation-id* (a unique identifier) as the message key to correlate messages for a transaction.

  For more information about this feature, see the "NRF Message Feed" section in *Oracle Communications Cloud Native Core, Network Repository Function User Guide*.

- **NRF Message Feed Enhancements**: The following additional message attributes are included in the metadata list, along with existing attributes:
  - source-ip
  - destination-ip
  - source-port
  - pod-instance-id
  - destination-port

  For more information about this feature, see the "NRF Message Feed" section in *Oracle Communications Cloud Native Core, Network Repository Function User Guide*.

- **NF Profile Size Limit**: This feature allows to specify the maximum limit of the NF Profile size that can be registered with NRF. The NF Profile size is evaluated during the `NfRegister` or `NfUpdate` service operation, and if the profile size is within the configured maximum limit, the service operation is allowed. If the profile size breaches the configured thresholds, the service operation gets rejected.
  For more information about this feature, see the "NF Profile Size Limit" section in *Oracle Communications Cloud Native Core, Network Repository Function User Guide.*

- **Pod Level Traffic Rejections (Overload Control Enhancements)**: With this enhancement, NRF rejects the incoming requests at pod level for percentage-based overload control by removing the dependency on cache-based coordination across pods. When the overload control level is breached, the number of requests to be rejected is calculated based on the requests received at each Ingress Gateway pod. This ensures a more accurate and consistent request rejection even in scenarios with low Transactions Per Second (TPS) and uneven traffic distribution.

  For more information about this feature, see the "Pod Level Traffic Rejections" section in *Oracle Communications Cloud Native Core, Network Repository Function User Guide.*

- **Support for cnDBTier Backup Status APIs in CNC Console**: With this enhancement, cnDBTier backup status APIs are integrated into the CNC Console. Users can view cnDBTier backup status APIs, such as the current timestamp, backup in progress, and next scheduled backup on CNC Console.
  For more information, see the "Support for cnDBTier APIs in CNC Console" section in *Oracle Communications Cloud Native Core, Network Repository Function User Guide*.

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

License Name	CCNC Number	Feature Name
Oracle Communications Cloud Native Core, Network Repository Function - 25K Active Subscribers Perpetual	CCNC-5363	NRF Message Feed Enhancements
Oracle Communications Cloud Native Core, Network Repository Function - 25K Active Subscribers Perpetual	CCNC-6080	Writing Messages of the Same Transaction in the Same Kafka Partition
Oracle Communications Cloud Native Core, Network Repository Function - 25K Active Subscribers Perpetual	CCNC-9424	Ingress Gateway Pod Protection Using Rate Limiting

2.8 Network Slice Selection Function (NSSF)

Release 25.1.200

Oracle Communications Cloud Native Core, Network Slice Selection Function (NSSF) 25.1.200 includes the following enhancements:

- **Support for Automated Certificate Lifecycle Management**: NSSF now supports integration with Oracle Communications Cloud Native Core, Certificate Management (OCCM) to enable automated TLS certificate lifecycle management. This integration simplifies the secure communication setup by automating the issuance, renewal, and management of certificates used for establishing TLS connections between network functions (NFs).
  For more information, see the "Support for Automated Certificate Lifecycle Management" section in *Oracle Communications Cloud Native Core, Network Slice Selection Function User Guide*.

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

Table 2-7 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-3632	Support for Automated Certificate Lifecycle Management

2.9 OCI Adaptor

Release 25.1.200

Oracle Communications Cloud Native Core, OCI Adaptor 25.1.200 includes the following enhancement:

- **Uplifted the OCI Adaptor Components**: The following OCI Adaptor components have been uplifted:
  - Management-agent is uplifted from 1.5.0 to 1.7.0.
  - Fluentd is uplifted from 1.5.0 to 1.6.0.
  - OTEL Collector is uplifted from 0.108.0 to 0.124.0.

2.10 Policy

Release 25.1.200

Oracle Communications Cloud Native Core, Converged Policy 25.1.200 includes the following enhancements:

- **Supports Reattempt after Back-off during N1N2 Communication**: PCF supports multiple N1N2 Communication attempts after backoff that would help in successful delivery of URSP rules to UE. For more information, see the "Support Backoff during N1N2 Communication" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.
- **Support for ASM 1.21.6:** Policy 25.1.200 supports Aspen Service Mesh (ASM) 1.21.6 version on Kubernetes 1.27 version from this release. For more information, see the "Configuring Policy to Support Aspen Service Mesh" section in *Oracle Communications Cloud Native Core, Policy Installation, Upgrade, and Fault Recovery Guide*.
- **Support for Dual Stack:** Using the dual stack mechanism, Policy communicates within services or deployments in a Kubernetes cluster using IPv4 or IPv6 or both simultaneously depending on the configured deployment mode. For more information about this feature, see the "Support for Dual Stack" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.
- **Support for NR vs EUTRA KPIs for N7 Interface***:* PCF application differentiate between NSA and SA call flows and provides KPI for N7 interface to differentiate between the NR and EUTRA radio access technology in the SM Service. The KPIs is visualized in Grafana dashboard. For more information, see the "Support for NR vs EUTRA KPIs for N7 Interface" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.
- **Pod protection by rate limiting at Ingress Gateway**: Policy supports configuring Rate Limiting for Ingress Gateway service in order to provide pod protection by throttling inbound requests, that exceeds the configured rate. For more information, see "Pod Protection at Ingress Gateway" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.
- **Supports Traffic Detection on SMF-N7 and TDF using Sd Interface**: PCF supports the Sd interface on Session Management Function (SMF)-N7 that enables it to communicate with the Traffic Detection Function (TDF). This interface allows PCF to provide Application Detection and Control (ADC) rules for traffic detection and enforcement at the TDF through Solicited Application Reporting. For more information, see the "Supports Traffic Detection on SMF-N7 and TDF using Sd Interface" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.

  > **Important**
  >
  > **Custom support for traffic detection on SMF-N7 and TDF using the Sd interface** is an experimental feature. It is subject to change and is not supported for production use (lab use only).

- **Modifying PCF Capacity parameters Through CNC Console**: This feature is updated to modify the capacity parameter of the PCF instance and Service instance in the NFProfile for PCF registration profile through CNC Console. For more information, see the "Integrating Policy with Different Network Functions" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide.*

- **Handling VoLTE Race Conditions Between AAR and STR Messages**: Policy now handles concurrency or collisions between Authorization Authentication Request (AAR-I/AAR-U) and Session Termination Request (STR) messages. It also addresses race conditions arising from Update Notify triggers due to AAR-I/AAR-U and STR for removing PCC rules. For more information, see the "Handling Collision Between AAR and STR Messages During Update Notify Timeout" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.
- **Handling of Multiple N1 N2 Transfer Messages:** If PCF receives more than one trigger while an N1N12 transfer is in progress and this feature is enabled, then it consolidates and stores the User Equipment Policy Set Identifiers (UPSIs) with UE Route Selection Policy (URSP) rules that needs to be transferred to UE. Once the UE notification is received for the in-progress N1N2 transfer, a final consolidation is performed. The consolidated UE policy actions are then sent to the UE in a single N1N2 transfer, assuming no fragmentation is required. Once the UE notification is received for the in-progress N1N2 transfer, final consolidation is performed and the consolidated UE policy actions are sent out to UE in a single (assuming no fragmentation is required) N1N2 transfer. For more information about this feature, see the "Handling of Multiple N1N2Transfer Messages" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.
- **Stale Binding Detection Audit, Report, and Recover**: Service disruptions caused by network storms, system overload, database latency, or other events can impact signaling between Policy and the Binding Support Function (BSF), affecting session bindings. Policy validates binding association records in its database for associated PDU sessions and checks if the binding association exists in BSF. If the binding association is missing in BSF, Policy initiates binding association registration with BSF and restores the session. For more information, see the "Stale Binding Detection Audit, Report and Recover" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.
- **Support for Reduced Capability UEs in SM-Rx Flows**: For voice and video calls by reduced capability devices on Voice over Long-Term Evolution (VoLTE) and Voice over New Radio (VoNR), Policy supports NR_REDCAP value for RAT Type over Rx interface. For more information, see the "Support for Handling Requests From Reduced Capability Devices" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.
- **LDAP Timeout and Retry Mechanism:** With this feature, Policy supports retry functionality towards external LDAP server. The operator must first enable the **Retry Enabled** flag to use this functionality. Then, the operator can configure the **Max number of retries** and **Retries on errors/timeout** to configure the multiple error codes including the error code for LDAP timeout (85). For more information about this feature, see the "LDAP Timeout and Retry Mechanism" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.
- **PCF support to not send ASR while Notify-Update fails:** This feature enables PCF to terminate a Policy Authorization/Rx session when it fails to update the required PCC (Policy and Charging Control) and session rules to the Session Management Function (SMF) for an Rx session of a PDU session. This lets the voice data packets or any other media type configured by user to be carried over default IMS QOS flow. For more information about this feature, see the "PCF support to not send ASR while Notify-Update fails" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.
- **Stale Requests Cleanup for Binding service**: Policy supports identifying and removing stale requests from SM service or PCRF Core to Binding service. Binding service stops further processing of such stale requests and responses and sends a 504 (Gateway Timeout) error to SM service or PCRF Core. For more information, see the "Support for Stale Requests Cleanup" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.

- **Stale Requests Cleanup for Diameter Connector**: Policy supports identifying and removing stale requests from Policy microservices such as SM service or PCRF Core to Diameter Connector. Diameter Connector stops further processing of such stale requests and responses and sends a 504 (Gateway Timeout) or 5454 error response SM service or PCRF Core. For more information, see the "Support for Stale Requests Cleanup" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.
- **Stale Requests Cleanup for User Service (CHF Connector or UDR Connector)**: Policy supports identifying and removing stale requests from PDS to User Service (UDR Connector or CHF Connector). User Service (UDR Connector or CHF Connector) stops further processing of such stale requests and responses and sends a 504 (Gateway Timeout response to PDS. For more information, see the "Support for Stale Requests Cleanup" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.
- **Stale Requests Cleanup for UE Policy service**: Policy supports identifying and removing stale requests from Ingress Gateway, PDS, PRE, or Bulwark service to UE Policy service. UE Policy service stops further processing of such stale requests and responses and sends a 504 (Gateway Timeout) error to Ingress Gateway, PDS, PRE, or Bulwark service. For more information, see the "Support for Stale Requests Cleanup" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.
- **Congestion Control Resource Usage Calculation Using EMA Algorithm:** The Congestion Control mechanism supports the Exponential Moving Average (EMA) algorithm for resource usage calculations. This algorithm calculates congestion resource usage by giving more weight to recent usage data, providing a more accurate representation of current resource utilization compared to a simple average across all data points. For more information, see the "Congestion Control Resource Usage Calculation Using EMA Algorithm" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.
- **Support for Pod Congestion Control**: Starting with Release 25.1.200, Policy now supports Pod Congestion Control across multiple services to manage heavy incoming request traffic. This mechanism evaluates each incoming request and decides whether to accept or reject it based on predefined request priority and the current congestion level of the service.
  - **User Service Pod Congestion Control**: The User service supports Pod Congestion Control to manage high volumes of incoming requests. For more information, see the "User Service Pod Congestion Control" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide.*
  - **Diameter Connector Pod Congestion Control**: The Diameter Connector service supports Pod Congestion Control to manage high volumes of incoming requests. For more information, see the "Diameter Connector Pod Congestion Control" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide.*
  - **Diameter Gateway Pod Congestion Control**: The Diameter Gateway service supports Pod Congestion Control to manage high volumes of incoming requests. This feature has been updated to align with the common Congestion Control mechanism. Users must migrate data from the older configuration parameters to the current common Congestion Control feature. For more information about the data migration, see the "Diameter Pod Congestion Control" and "Congestion Control settings" sections in *Oracle Communications Cloud Native Core, Converged Policy User Guide.*
  - **AM Service Pod Congestion Control**: The AM service supports Pod Congestion Control to manage high volumes of incoming requests For more information, see the "AM Service Pod Congestion Control" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.

  - **Notifier Service Pod Congestion Control**: The Notifier service supports Pod Congestion Control to manage high volumes of incoming requests. It considers every incoming request and decides to either reject or accept it based on a defined request priority and the status of service congestion level. For more information, see the "Notifier Service Pod Congestion Control" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.

- **Single UE ID Implementation**: Policy supports optimizing the query on PolicyDS database using configurable UE IDs. Also, Policy reports on the migration status of database records when the query type is switched based on UE IDs. For example, it reports the number of database records to be migrated when switching from Multi UE ID to Single UE ID. For more information, see "Optimizing PolicyDS Database Query With Configurable UE IDs" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.
- **Histogram Metrics for Signaling and DB Access Processing Latency in Binding Service**: In order to provide sufficient insight into Binding service's performance for incoming requests, Policy includes histogram metrics for Binding service. These Histogram metrics enable Policy to observe data distribution by measuring the latency of multiple HTTP and database requests sent and received by Binding service. For more information, see the "Support for Signaling and DB Access Processing Latency Histogram Metrics" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.
- **Handling DB cluster disconnect**: PCF Cluster DB State API is integrated with CNC Console for Policy, which enables to view the PCF cluster database state on cnDBTier database. This API displays the realtime status of the cluster state and NF database functional state in the cnDBTier database cluster. For more information, see the "Support for cnDBTier APIs in CNC Console" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.
- **Enhanced Logging Support for Error Responses:** Policy has been enhanced to support verbose logging for microservices involved in SM call flows (create, update, delete, and notify) at their default log level (WARN) to provide sufficient visibility into issues within or across the external facing interfaces of the microservices. For more information about this feature, see the "Logging Support for Error Response" section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.

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

License Name	CCNC Number	Feature Name
Oracle Communications Cloud Native Core, Policy Control Function - 25K Active Subscribers Perpetual	CCNC-9713	Supports Reattempt after Back-off during N1N2 Communication
Oracle Communications Cloud Native Core, Policy Control Function - 25K Active Subscribers Perpetual	CCNC-9615	Support for ASM 1.21.6
Oracle Communications Cloud Native Core, Policy and Charging Rules Function - per 25K Subscribers Perpetual	CCNC-9392 and CCNC-4995	Support for Dual Stack
Oracle Communications Cloud Native Core, Policy Control Function - 25K Active Subscribers Perpetual	CCNC-9173	Support for NR vs EUTRA KPIs for N7 Interface
Oracle Communications Cloud Native Core, Policy Control Function - 25K Active Subscribers Perpetual	CCNC-9108	Pod protection by rate limiting at Ingress Gateway

License Name	CCNC Number	Feature Name
Oracle Communications Cloud Native Core, Policy and Charging Rules Function - per 25K Subscribers Perpetual	CCNC-9088	Supports Traffic Detection on SMF-N7 and TDF using Sd Interface
Oracle Communications Cloud Native Core, Policy Control Function - 25K Active Subscribers Perpetual	CCNC-8499	Integrating Policy with Different Network Functions
Oracle Communications Cloud Native Core, Policy Control Function - 25K Active Subscribers Perpetual	CCNC-8399	VoLTE Race Condition - Handling collision between AAR-STR, with UpdateNotify time out
Oracle Communications Cloud Native Core, Policy Control Function - 25K Active Subscribers Perpetual	CCNC-8176	PCF support to not send ASR while Notify-Update fails
Oracle Communications Cloud Native Core, Policy and Charging Rules Function - per 25K Subscribers Perpetual	CCNC-6293	LDAP Timeout and Retry Mechanism
Oracle Communications Cloud Native Core, Policy Control Function - 25K Active Subscribers	CCNC-8304	Handling of Multiple N1 N2 Transfer Messages
Oracle Communications Cloud Native Core, Policy Control Function - 25K Active Subscribers	CCNC-8725	PCF and BSF stale Binding Detection AUDIT and Report and Recover

2.11 Service Communication Proxy (SCP)

Release 25.1.201

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

Release 25.1.200

Oracle Communications Cloud Native Core, Service Communication Proxy (SCP) 25.1.200 includes the following enhancements:

- **Support for ASM 1.21.6**: SCP supports Aspen Service Mesh (ASM) 1.21.6 from this release. For more information, see the "Configuring SCP to Support Aspen Service Mesh" section in *Oracle Communications Cloud Native Core, Service Communication Proxy Installation, Upgrade, and Fault Recovery Guide*.
- **Support for Dual Stack**: This enhancement introduces dual stack support for Aspen Service Mesh (ASM). For more information, see the "Support for Dual Stack" section in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.
- **Verbose Logging for SCP**: This enhancement introduces verbose logging specifically for the SCP-Cache microservice within the data plane. For more information, see the "Verbose Logging for SCP" section in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.
- **Enhanced Notifications Handling**: With the Enhanced Notifications Handling feature, SCP can alternate route notification requests even if the 3gpp-Sbi-Routing-Binding header does not contain the `servName` attribute. SCP obtains the target producer NF information from `nfset` and `nfinst` attributes of the notification request. In this case, SCP pegs the exact values of the producer NF type in `ocscp_nf_type` and `ocscp_nf_service_type` dimensions of the respective metrics. For more information, see the "Enhanced Notification

Handling" and "Obtaining NF Information from Notification Requests" sections in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.

- **Application Framework Change**: Spring Boot has been replaced with Micronaut as the framework for microservices. To facilitate internal communication between SCP microservices, the following services have been introduced:
  - <helm-release-name>-scp-worker-int: Handles internal Server-Sent Events (SSE) communications for SCP-Worker, specifically for requests initiated towards Network Repository Function (NRF) from SCP-nrfProxy and SCP-nrfProxy-oauth services for Model-D and OAuth.
  - Additional "-int" services: Manage all other internal SSE communications, except those handled by scp-worker-int, between corresponding non "-int" services. The following "-int" services are supported:
    * <helm-release-name>-scpc-alternate-resolution-int
    * <helm-release-name>-scpc-audit-int
    * <helm-release-name>-scpc-configuration-int
    * <helm-release-name>-scpc-notification-int

    <helm-release-name> will be prefixed in each service name. For example, if the Helm release name is ocscp, then the scpc-configuration-int microservice name will be "ocscp-scpc-configuration-int".

  This architecture ensures streamlined and efficient internal communication within the SCP microservices. You must exclude the service ports of these services while configuring ASM. For more information about service ports, see the "SCP Traffic IP Flow" section in *Oracle Communications Cloud Native Core, Service Communication Proxy Installation, Upgrade, and Fault Recovery Guide*.

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

Table 2-8 License names for feature mapping

License Name	CCNC Number	Feature Name
Oracle Communications Cloud Native Core, Service Communication Proxy - 25K Active Subscribers Perpetual	CCNC-9671	Application Framework Change
Oracle Communications Cloud Native Core, Service Communication Proxy - 25K Active Subscribers Perpetual	CCNC-8832	Support for ASM 1.21.6
Oracle Communications Cloud Native Core, Service Communication Proxy - 25K Active Subscribers Perpetual	CCNC-8122	Enhanced Notifications Handling
Oracle Communications Cloud Native Core, Service Communication Proxy - 25K Active Subscribers Perpetual	CCNC-7610	Obtaining NF Information from Notification Requests
Oracle Communications Cloud Native Core, Advance Networking - 25K Active Subscribers	CCNC-5190	Support for Dual Stack
Oracle Communications Cloud Native Core, Service Communication Proxy - 25K Active Subscribers Perpetual	CCNC-5169	Verbose Logging for SCP

Table 2-8 (Cont.) License names for feature mapping

License Name	CCNC Number	Feature Name
Oracle Communications Cloud Native Core, Service Communication Proxy - 25K Active Subscribers Perpetual	CCNC-3627	Model-D Capacity Enhancement

2.12 Security Edge Protection Proxy (SEPP)

Release 25.1.201

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

Release 25.1.200

Oracle Communications Cloud Native Core, Security Edge Protection Proxy (SEPP) 25.1.200 includes the following enhancements:

- **Cat-1 NRF Service API Query Parameters Validation:**
  With this feature, SEPP supports filtering of request based on the specific NF Type combination.

  This feature leverages the requester-nf-type and target-nf-type details provided in the discovery request, allowing operators to configure and enforce fine-grained control over Cat-1 rules.

  Key benefits of the feature includes:

  - Controlled access: Restricts access to the nnrf-disc service based on NF types, blocking unauthorized requests.
  - Improved security: Blocks unapproved access, improves security and protects the system from unwanted or harmful interactions.
  - Targeted filtering: Enables operators to define rules based on NF types, providing precise control over which network functions can access the service.
  - Reduced risk: Acts as a firewall to reduce the chances of untrusted network functions connecting to important APIs, making the system safer.
    This feature enhances security by allowing only trusted network functions to access the NNRF-disc service.

    For more information, see the "Cat-1 NRF Service API Query Parameters Validation Feature" section in *Oracle Communications Cloud Native Core, Security Edge Protection Proxy User Guide*, *Oracle Communications Cloud Native Core, Security Edge Protection Proxy REST Specification Guide*, and *Oracle Communications Cloud Native Core, Security Edge Protection Proxy Troubleshooting Guide*.
- **LCI and OCI Headers in 5G Architecture:** In the 5G architecture, frequent network overload due to substantial data exchanges between producer and consumer Network Functions (NFs) necessitates precise load balancing to prevent failures. Prompt communication of overload conditions from producer NFs to consumer NFs is essential for timely corrective actions. The LCI and OCI headers play a critical role by providing real-time insights into SEPP resources and facilitating efficient traffic management. These headers equip consumer NFs with critical load and overload information, optimizing traffic distribution and proactive measures during overload scenarios, ensuring a stable, high-performing 5G Core Network, even under heavy loads. For more information, see the "LCI and OCI Headers" section in *Oracle Communications Cloud Native Core, Security Edge*

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

- **SEPP Dashboard Support for Detecting Vulnerable Messages:**
  In earlier releases, SEPP metrics could not be filtered by the originating PLMN ID, making it difficult to segregate and identify the source of messages. This feature enhances the metrics by enabling segregation based on PLMN ID, thereby improving operational efficiency in tracking message origins.
  - **CSEPP**: The existing metric ocsepp_cn32f_requests_total has been enhanced to include source_plmn_id as a new dimension.
  - **PSEPP**: A new metric ocsepp_originating_network_request_success_total has been introduced, which includes peer_plmn as a dimension.

  For more information, see the "SEPP Dashboard Support for Detecting Vulnerable Messages" section in *Oracle Communications Cloud Native Core, Security Edge Protection Proxy User Guide*.

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

Table 2-9 License names for feature mapping

License Name	CCNC Number	Feature Name
Oracle Communications Cloud Native Core, 5G Signaling Firewall - 25K Active Subscribers Perpetua	CCNC-6385	Cat-1 NRF Service API Query Parameters Validation
Oracle Communications Cloud Native Core, Security Edge Protection Proxy - 25K Active Subscribers Perpetual	CCNC-3460	LCI and OCI Headers
Oracle Communications Cloud Native Core, Security Edge Protection Proxy - 25K Active Subscribers Perpetual	CCNC-4307	SEPP Dashboard Support for Detecting Vulnerable Messages

2.13 Unified Data Repository (UDR)

Release 25.1.200

Oracle Communications Cloud Native Core, Unified Data Repository (UDR) 25.1.200 includes the following enhancements:

- **Lifecycle Management (LCM) Based Automation**: This feature optimizes the deployment or upgrade steps. This is achieved by automating service account creation that enables you to create user-defined service account automatically without performing any manual steps. For more information, see the "Lifecycle Management (LCM) Based Automation" section in *Oracle Communications Cloud Native Core, Unified Data Repository User Guide* and *Oracle Communications Cloud Native Core, Provisioning Gateway Installation Guide*.
- **Support for Export of Policy Data in Comma Separated Value (CSV) Format**: This feature enables the Subscriber Export Tool to export the 5G and 4G subscriber policy data, which includes the profile data and policy data (*am-data, sm-data, and ue-policy-set*) in CSV file format from cnUDR. The converted subscriber data in CSV file format is used by the Subscriber Bulk Import Tool to import the subscriber data along with its policy data on an another instance of cnUDR. For more information, see the "Support for Export of Policy

Data in Comma Separated Value (CSV) Format" section in *Oracle Communications Cloud Native Core, Unified Data Repository User Guide*.

- **Support for Dual Stack**: With this feature, cnUDR and Provisioning Gateway can be deployed on a dual stack Kubernetes infrastructure. Using the dual stack mechanism, cnUDR and Provisioning Gateway establish and accept connections within pods and services in a Kubernetes cluster using IPv4 or IPv6. For more information, see the "Support for Dual Stack" section in *Oracle Communications Cloud Native Core, Unified Data Repository User Guide* and *Oracle Communications Cloud Native Core, Provisioning Gateway Installation Guide*.
- **Support for cnDBTier Backup Status APIs in CNC Console**: With this enhancement, UDR can view the cnDBTier backup status, such as the current timestamp, backup in progress, and next scheduled backup using CNC Console. For more information, see the "cnDBTier Backup Status" section in *Oracle Communications Cloud Native Core, Unified Data Repository User Guide*.
- **Ingress Gateway Pod Protection Using Rate Limiting**: With this feature, rate limiting mechanism is applied for Ingress Gateway pods. This mechanism allows pods to process a predefined number of requests. When the request rate exceeds the threshold, the pods take action to protect themselves. Depending on the configuration, the pods either reject the additional requests with a custom error code or allows the request. For more information, see the "Ingress Gateway Pod Protection Using Rate Limiting" section in *Oracle Communications Cloud Native Core, Unified Data Repository User Guide*.
- **Support for ASM 1.21.6:** UDR 25.1.200 supports Aspen Service Mesh (ASM) 1.21.6 version on Kubernetes 1.27 version from this release. For more information, see the "Configuring UDR to Support Aspen Service Mesh" section in *Oracle Communications Cloud Native Core, Unified Data Repository 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 2-10 License names for feature mapping

License Name	CCNC Number	Feature Name
Oracle Communications Cloud Native Core, Subscriber Location Function - 25K Active Subscribers Perpetual	CCNC-10117	SLF capacity growth on 23.4.1 (Signalling TPS = 50K ; Provisioning TPS = 1.2K , Sub Cap: 64M)
Oracle Communications Cloud Native Core, Advance Networking - 25K Active Subscribers	CCNC-9467	Support for Dual Stack
Oracle Communications Cloud Native Core, Automated Lifecycle Management - 25K Active Subscribers	CCNC-9151	Lifecycle Management (LCM) Based Automation
Oracle Communications Cloud Native Core, Subscriber Location Function - 25K Active Subscribers Perpetual	CCNC-9133	Support for ASM 1.21.6
Oracle Communications Cloud Native Core, Automated Lifecycle Management - 25K Active Subscribers	CCNC-9094	Lifecycle Management (LCM) Based Automation
Oracle Communications Cloud Native Core, Unified Data Repository - 25K Active Subscribers Perpetual	CCNC-5480	Support for Export of Policy Data in Comma Separated Value (CSV) Format

Table 2-10 (Cont.) License names for feature mapping

License Name	CCNC Number	Feature Name
Oracle Communications Cloud Native Core, Unified Data Repository - 25K Active Subscribers	-	Ingress Gateway Pod Protection Using Rate Limiting

3
Media and Documentation

3.1 Media Pack

This section lists the media package for Oracle Communications Cloud Native Core 3.25.1.2xx.0. To download the media package, see MOS.

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

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

Table 3-1 Media Pack Contents for Oracle Communications Cloud Native Core 3.25.1.2xx.0

Description	NF Version	ATS Version	Upgrade Supported
Oracle Communications Cloud Native Core, Binding Support Function (BSF)	25.1.200	25.1.200	BSF 25.1.200 supports fresh installation and upgrade from 24.2.x and 24.1.x. For more information, see *Oracle Communications Cloud Native Core, Binding Support Function Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Configuration Console (CNC Console)	25.1.200	NA	CNC Console 25.1.200 supports fresh installation and upgrade from 25.1.1xx, 24.3.x and 24.2.x. For more information, see *Oracle Communications Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Certificate Management (OCCM)	25.1.200	NA	OCCM 25.1.200 supports fresh installation and upgrade from 25.1.1xx and 24.3.x. For more information, see *Oracle Communications Cloud Native Core, Certificate Management Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, OCI Adaptor	25.1.200	NA	OCI Adaptor 25.1.200 supports fresh installation only. For more information, see *Oracle Communications Cloud Native Core, OCI Deployment Guide*.

Table 3-1 (Cont.) Media Pack Contents for Oracle Communications Cloud Native Core 3.25.1.2xx.0

Description	NF Version	ATS Version	Upgrade Supported
Oracle Communications Cloud Native Core, Cloud Native Environment (CNE)	25.1.200	NA	CNE 25.1.200 supports fresh installation and upgrade from 25.1.1xx. For more information, see *Oracle Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide.*
Oracle Communications Operations Services Overlay (OSO)	25.1.200	NA	OSO 25.1.200 supports fresh installation and upgrade from 25.1.1xx. For more information, see *Oracle Communications Cloud Native Core, Operations Services Overlay Installation and Upgrade Guide*.
Oracle Communications Cloud Native Core, cnDBTier (cnDBTier)	25.1.201	NA	cnDBTier 25.1.201 supports fresh installation and upgrade from 25.1.1xx and 24.3.x. For more information, see *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, cnDBTier (cnDBTier)	25.1.200	NA	cnDBTier 25.1.200 supports fresh installation and upgrade from 25.1.1xx and 24.3.x. For more information, see *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Network Repository Function (NRF)	25.1.200	25.1.200	NRF 25.1.200 supports fresh installation and upgrade from 25.1.1xx and 24.3.x. For more information, see *Oracle Communications Cloud Native Core, Network Repository Function Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Network Slice Selection Function (NSSF)	25.1.200	25.1.200	NSSF 25.1.200 supports fresh installation and upgrade from 25.1.1xx. For more information, see *Oracle Communications Cloud Native Core, Network Slice Selection Function Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Converged Policy (Policy)	25.1.200	25.1.200	Policy 25.1.200 supports fresh installation and upgrade from 24.2.x and 24.1.x. For more information, see *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide*.

Table 3-1 (Cont.) Media Pack Contents for Oracle Communications Cloud Native Core 3.25.1.2xx.0

Description	NF Version	ATS Version	Upgrade Supported
Oracle Communications Cloud Native Core, Service Communications Proxy (SCP)	25.1.201	25.1.201	SCP 25.1.201 supports fresh installation and upgrade from 25.1.1xx and 24.3.x. For more information, see *Oracle Communications Cloud Native Core, Service Communication Proxy Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Service Communications Proxy (SCP)	25.1.200	25.1.200	SCP 25.1.200 supports fresh installation and upgrade from 25.1.1xx and 24.3.x. For more information, see *Oracle Communications Cloud Native Core, Service Communication Proxy Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Security Edge Protection Proxy (SEPP)	25.1.201	25.1.201	SEPP 25.1.201 supports fresh installation and upgrade from 25.1.200, 25.1.1xx, and 24.3.x. For more information, see *Oracle Communications Cloud Native Core, Security Edge Protection Proxy Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Security Edge Protection Proxy (SEPP)	25.1.200	25.1.200	SEPP 25.1.200 supports fresh installation and upgrade from 25.1.1xx and 24.3.x. For more information, see *Oracle Communications Cloud Native Core, Security Edge Protection Proxy Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Security Edge Protection Proxy (SEPP)	25.1.200	25.1.200	SEPP 25.1.200 supports fresh installation and upgrade from 25.1.1xx and 24.3.x. For more information, see *Oracle Communications Cloud Native Core, Security Edge Protection Proxy Installation, Upgrade, and Fault Recovery Guide*.
Oracle Communications Cloud Native Core, Unified Data Repository (UDR)	25.1.200	25.1.200	UDR 25.1.200 supports fresh installation and upgrade from 25.1.1xx and 24.3.x. For more information, see *Oracle Communications Cloud Native Core, Unified Data Repository Installation, Upgrade, and Fault Recovery Guide*.

Cloud Native Core Upgrade

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

Figure 3-1 Cloud Native Core Upgrade

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

Note

***** Policy, CNCC, 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). 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	26.1.1xx	26.1.2xx	26.2.1xx	26.2.2xx
24.2. x	Y	NS	NS	NS	NS	NS	NS	NS	NS
24.3. x	NA	Y	NS	NS	NS	NS	NS	NS	NS
25.1.1xx	NA	NA	Y	NS	NS	NS	NS	NS	NS
25.1.2xx	NA	NA	NA	Y	NS	NS	NS	NS	NS
25.2.1xx	NA	NA	NA	NA	Y	NS	NS	NS	NS
25.2.2xx	NA	NA	NA	NA	NA	Y	NS	NS	NS
26.1.1xx	NA	NA	NA	NA	NA	NA	Y	NS	NS
26.1.2xx	NA	NA	NA	NA	NA	NA	NA	Y	NS
26.2.1xx	NA	NA	NA	NA	NA	NA	NA	NA	Y
26.2.2xx	NA	NA	NA	NA	NA	NA	NA	NA	NA

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

3.2 Compatibility Matrix

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

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

Table 3-2 Compatibility Matrix

CNC NF	NF Version	CNE	cnDBTier	OSO	ASM S/W	Kubernetes	CNC Console	OCNADD	OCCM	OCI Adaptor
BSF*	25.1.200	• 25.1.2xx • 25.1.1xx • 24.3.x	• 25.1.2xx • 25.1.1xx • 24.3.x	• 25.1.2xx • 25.1.1xx • 24.3.x	• 1.21.6 • 1.14.6 • 1.11.8	• 1.32.x • 1.31.x • 1.30.x	25.1.2xx	NA	NA	NA
CNC Console*	25.1.200	• 25.1.2xx • 25.1.1xx • 24.3.x • 24.2.x	• 25.1.2xx • 25.1.1xx • 24.3.x • 24.2.x	• 25.1.2xx • 25.1.1xx • 24.3.x • 24.2.x	• 1.21.6 • 1.14.6 • 1.11.8 • 1.9.8	• 1.32.x • 1.31.x • 1.30.x	NA	25.1.2xx	25.1.2xx	25.1.2xx
cnDBTier	25.1.201	• 25.1.2xx • 25.1.1x • 24.3.x	NA	NA	NA	• 1.32.x • 1.31.x • 1.30.x	NA	NA	NA	NA
cnDBTier*	25.1.200	• 25.1.200 • 25.1.1x • 24.3.x	NA	NA	NA	• 1.32.x • 1.31.x • 1.30.x	NA	NA	NA	NA
CNE	25.1.200	NA	NA	NA	NA	1.32.x	NA	NA	NA	NA

Table 3-2 (Cont.) Compatibility Matrix

CNC NF	NF Version	CNE	cnDBTier	OSO	ASM S/W	Kubernetes	CNC Console	OCNADD	OCCM	OCI Adaptor
NRF*	25.1.200	• 25.1.2xx • 25.1.1xx • 24.3.x	• 25.1.2xx • 25.1.1xx • 24.3.x	• 25.1.2xx • 25.1.1xx • 24.3.x	1.14.6	• 1.32.x • 1.31.x • 1.30.x	25.1.2xx	25.1.2xx	25.1.2xx	25.1.2xx
NSSF	25.1.200	• 25.1.2xx • 25.1.1xx • 24.3.x	• 25.1.2xx • 25.1.1xx • 24.3.x	• 25.1.2xx • 25.1.1xx • 24.3.x	1.14.6	• 1.32.x • 1.31.x • 1.30.x	25.1.2xx	NA	NA	NA
OCCM	25.1.200	• 25.1.2xx • 25.1.1x • 24.3.x	NA	NA	NA	• 1.32.x • 1.31.x • 1.30.x	25.1.2xx	NA	NA	NA
OCI Adaptor	25.1.200	NA	NA	NA	NA	• 1.32.x • 1.31.x • 1.30.x	NA	NA	NA	NA
OSO*	25.1.200	NA	NA	NA	NA	• 1.32.x • 1.31.x • 1.30.x	NA	NA	NA	NA
Policy*	25.1.200	• 25.1.2xx • 24.3.x • 24.2.x	• 25.1.2xx • 24.3.x • 24.2.x	• 25.1.2xx • 24.3.x • 24.2.x	• 1.21.6 • 1.14.6 • 1.11.8	• 1.32.x • 1.30.x • 1.29.x	25.1.2xx	NA	NA	NA

Table 3-2 (Cont.) Compatibility Matrix

CNC NF	NF Version	CNE	cnDBTier	OSO	ASM S/W	Kubernetes	CNC Console	OCNADD	OCCM	OCI Adaptor
SCP*	25.1.201	• 25.1.2xx • 25.1.1xx • 24.3.x	• 25.1.2xx • 25.1.1xx • 24.3.x	• 25.1.2xx • 25.1.1xx • 24.3.x	• 1.21.6 • 1.14.6 • 1.11.8	• 1.32.x • 1.31.x • 1.30.x	25.1.2xx	25.1.2xx	25.1.2xx	25.1.2xx
SCP*	25.1.200	• 25.1.2xx • 25.1.1xx • 24.3.x	• 25.1.2xx • 25.1.1xx • 24.3.x	• 25.1.2xx • 25.1.1xx • 24.3.x	• 1.21.6 • 1.14.6 • 1.11.8	• 1.32.x • 1.31.x • 1.30.x	25.1.2xx	25.1.2xx	25.1.2xx	25.1.2xx
SEPP*	25.1.201	• 25.1.2xx • 25.1.1xx • 24.3.x	• 25.1.2xx • 25.1.1xx • 24.3.x	• 25.1.2xx • 25.1.1xx • 24.3.x	• 1.21.6 • 1.14.6 • 1.11.8	• 1.32.x • 1.31.x • 1.30.x	25.1.2xx	25.1.2xx	25.1.2xx	25.1.2xx
SEPP*	25.1.200	• 25.1.2xx • 25.1.1xx • 24.3.x	• 25.1.2xx • 25.1.1xx • 24.3.x	• 25.1.2xx • 25.1.1xx • 24.3.x	• 1.21.6 • 1.14.6 • 1.11.8	• 1.32.x • 1.31.x • 1.30.x	25.1.2xx	25.1.2xx	25.1.2xx	25.1.2xx

Table 3-2 (Cont.) Compatibility Matrix

CNC NF	NF Version	CNE	cnDBTier	OSO	ASM S/W	Kubernetes	CNC Console	OCNADD	OCCM	OCI Adaptor
UDR*	25.1.200	• 25.1.2xx • 25.1.1xx • 24.3.x	• 25.1.2xx • 25.1.1xx • 24.3.x	• 25.1.2xx • 25.1.1xx • 24.3.x	• 1.21.6 • 1.14.6 • 1.11.8	• 1.32.x • 1.31.x • 1.30.x	25.1.2xx	NA	25.1.2xx	NA

> **Note**
>
> *: Kubernetes 1.20.x and 1.25.x versions are only supported for ASM based deployment.

3.3 3GPP Compatibility Matrix

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

Table 3-3 3GPP Compatibility Matrix

CNC NF	NF Version	3GPP
BSF	25.1.200	• 3GPP TS 23.501 v17.7.0 • 3GPP TS 23.502 v17.7 • 3GPP TS 23.503 V17.7 • 3GPP TS 29.500 v17.7.0 • 3GPP TS 29.510 v17.7 • 3GPP TS 29.513 V17.7 • 3GPP TS 29.521 v17.7.0 • 3GPP TS 33.501 V17.7.0
CNC Console	25.1.200	NA
cnDBTier	25.1.2xx	NA
CNE	25.1.200	NA
NRF	25.1.200	• 3GPP TS 29.510 v15.5 • 3GPP TS 29.510 v16.3.0 • 3GPP TS 29.510 v16.7 • 3GPP TS 29.510 v17.7
NSSF	25.1.200	• 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

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

CNC NF	NF Version	3GPP
OCCM	25.1.200	• 3GPP TS 33.310-h30 • 3GPP TR 33.876 v.0.3.0
OSO	25.1.200	NA
OCI Adaptor	25.1.200	NA
Policy	25.1.200	• 3GPP TS 33.501 v17.7.0 • 3GPP TS 29.500v16.9.0 • 3GPP TS 23.501v16.9.0 • 3GPP TS 23.502v16.9.0 • 3GPP TS 23.503v16.9.0 • 3GPP TS 29.504v16.9.0 • 3GPP TS 29.507v16.9.0 • 3GPP TS 29.510v16.9.0 • 3GPP TS 29.512v16.14 • 3GPP TS 29.513v16.9.0 • 3GPP TS 29.514v16.14.0 • 3GPP TS 29.214v16.5.0 • 3GPP TS 29.518v16.13.0 • 3GPP TS 29.519v16.8 • 3GPP TS 29.520v16.8 • 3GPP TS 29.521v16.8.0 • 3GPP TS 29.525v16.9.0 • 3GPP TS 29.594v16.7 • 3GPP TS 23.203 v16.2.0 • 3GPP TS 29.212 V16.3.0 • 3GPP TS 29.213v16.3 • 3GPP TS 29.214 v16.2.0 • 3GPP TS 29.219 v16.0.0 • 3GPP TS 29.335v16.0
SCP	25.1.2xx	3GPP TS 29.500 v17.12.0
SEPP	25.1.2xx	• 3GPP TS 23.501 v17.6.0 • 3GPP TS 23.502 v17.6.0 • 3GPP TS 29.500 v17.8.0 • 3GPP TS 29.501 v17.7.0 • 3GPP TS 29.573 v17.6.0 • 3GPP TS 29.510 v17.7.0 • 3GPP TS 33.501 v17.7.0 • 3GPP TS 33.117 v17.1.0 • 3GPP TS 33.210 v17.1.0
UDR	25.1.200	• 3GPP TS 29.505 v15.4.0 • 3GPP TS 29.504 v16.2.0 • 3GPP TS 29.519 v16.2.0 • 3GPP TS 29.511 v17.2.0

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

3.4 Common Microservices Load Lineup

This section provides information about common microservices and ATS for the specific NF versions in Oracle Communications Cloud Native Core Release 3.25.1.2xx.0.

Table 3-4 Common Microservices Load Lineup for Network Functions

CNC NF	NF Version	Alternate Route Svc	App-Info	ASM Configuration	ATS Framework	Config-Server	Debug-tool	Egress Gateway	Ingress Gateway	Helm Test	Mediation	NRF-Client	Perf-Info
BSF	25.1.200	25.1.203	25.1.201	25.1.200	25.1.201	25.1.201	25.1.202	25.1.203	25.1.203	25.1.201	NA	25.1.202	25.1.201
CNC Console	25.1.200	NA	NA	NA	NA	NA	25.1.202	NA	25.1.203	25.1.201	NA	NA	NA
OCCM	25.1.200	NA	NA	NA	NA	NA	25.1.202	NA	NA	25.1.201	NA	NA	NA
NRF	25.1.200	25.1.203	25.1.201	25.1.201	25.1.202	NA	25.1.202	25.1.203	25.1.203	25.1.201	NA	NA	25.1.201
NSSF	25.1.200	25.1.203	25.1.201	25.1.200	25.1.202	25.1.201	25.1.202	25.1.203	25.1.203	25.1.201	NA	25.1.202	25.1.201
Policy	25.1.200	25.1.203	25.1.201	25.1.200	25.1.201	25.1.201	25.1.202	25.1.203	25.1.203	25.1.201	NA	25.1.202	25.1.201
SCP	25.1.201	NA	NA	25.1.201	25.1.202	NA	25.1.202	NA	NA	25.1.201	25.1.200	NA	NA
SCP	25.1.200	NA	NA	25.1.201	25.1.202	NA	25.1.202	NA	NA	25.1.201	25.1.200	NA	NA
SEPP	25.1.201	25.1.204	25.1.202	25.1.201	25.1.202	25.1.202	25.1.202	25.1.204	25.1.204	25.1.201	25.1.105	25.1.202	25.1.202
SEPP	25.1.200	25.1.203	25.1.202	25.1.201	25.1.202	25.1.202	25.1.202	25.1.203	25.1.203	25.1.201	25.1.105	25.1.202	25.1.202
UDR	25.1.200	25.1.203	25.1.201	25.1.201	25.1.202	25.1.201	25.1.202	25.1.203	25.1.203	25.1.201	NA	25.1.202	25.1.201

3.5 Generic Open Source Software Compatibility on Any Platform

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

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

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

Software	Tested Software Version			Software Requirement	Category	Sub-Category	Category Requirement	Usage Description
	NF 25.1.2xx	NF 25.1.1xx	NF 24.3.x					
Kubernetes	1.32.0	1.31	1.30	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 3-5 (Cont.) Generic Open Source Software Compatibility on Any Platform

Software	Tested Software Version			Software Requirement	Category	Sub-Category	Category Requirement	Usage Description
	NF 25.1.2xx	NF 25.1.1xx	NF 24.3.x					
Helm	3.17.1	3.16.2	3.15.2	Mandatory	Management	Kubernetes Package Management	Mandatory	Helm, a package manager, simplifies deploying and managing NFs on Kubernetes with reusable, versioned charts for easy automation and scaling. **Impact**: Preinstallation is required. Not using this capability may result in error-prone and time-consuming management of NF versions and configurations, impacting deployment consistency.
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	1.7.24	1.7.22	1.7.16	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 3-5 (Cont.) Generic Open Source Software Compatibility on Any Platform

Software	Tested Software Version			Software Requirement	Category	Sub-Category	Category Requirement	Usage Description
	NF 25.1.2xx	NF 25.1.1xx	NF 24.3.x					
Velero	1.13.2	1.13.2	1.12.0	Recommended	Backup	Backup and Disaster Recovery for Kubernetes	Optional	Velero backs up and restores Kubernetes clusters for 5G NFs, ensuring data protection and disaster recovery. **Impact**: Without backup and recovery capabilities, customers would risk data loss and extended downtime, requiring a full cluster reinstall in case of failure or upgrade.
Kyverno	1.13.4	1.12.5	1.12.5	Recommended	Security	Kubernetes Policy Management	Mandatory	Kyverno is a Kubernetes policy engine that allows to manage and enforce policies for resource configurations within a Kubernetes cluster. **Impact**: Failing to implement policy enforcement could lead to misconfigurations, resulting in security risks and instability in NF operations, affecting reliability.
MetalLB	0.14.4	0.14.4	0.14.4	Recommended	Networking	Load Balancer for Kubernetes	Mandatory	MetalLB provides load balancing and external IP management for 5G NFs in Kubernetes environments. **Impact**: MetalLB is used as LB solution in CNE. LB is mandatory for the solution to work. Without load balancing, traffic distribution among NFs may be inefficient, leading to potential bottlenecks and service degradation.

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

Software	Tested Software Version			Software Requirement	Category	Sub-Category	Category Requirement	Usage Description
	NF 25.1.2xx	NF 25.1.1xx	NF 24.3.x					
CoreDNS	1.11.13	1.11.1	1.11.1	Recommended	Networking	Service Discovery for Kubernetes	Mandatory	CoreDNS is the DNS server in Kubernetes, which provides DNS resolution services within the cluster. **Impact**: DNS is an essential part of deployment. Without proper service discovery, NFs would struggle to communicate with each other, leading to connectivity issues and operational failures.
Multus	4.1.3	3.8	3.8.0	Recommended	Networking	Networking for Kubernetes traffic segregation	Conditional	Multus enables multiple network interfaces in Kubernetes pods, allowing custom configurations and isolated paths for advanced use cases such as NF deployments, ultimately supporting traffic segregation. **Impact**: Without this capability, connecting NFs to multiple networks could be limited, impacting network performance and isolation.

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

Software	Tested Software Version			Software Requirement	Category	Sub-Category	Category Requirement	Usage Description
	NF 25.1.2xx	NF 25.1.1xx	NF 24.3.x					
Fluentd	1.17.1	1.17.1	1.16.2	Recommended	Logging	Logging Agent	Mandatory	Fluentd is an open-source data collector that streamlines data collection and consumption, allowing for improved data utilization and comprehension. **Impact**: Not utilizing centralized logging can hinder the ability to track NF activity and troubleshoot issues effectively, complicating maintenance and support.
OpenSearch	2.15.0	2.11.0	2.11.0	Recommended	Logging	Search/ Analytics / Logging	Mandatory	OpenSearch provides scalable search and analytics for 5G NFs, enabling efficient data exploration and visualization. Lack of a robust analytics solution could lead to challenges in identifying performance issues and optimizing NF operations, affecting overall service quality.
OpenSearch Dashboard	2.15.0	2.11.0	2.11.0	Recommended	Logging	Dashboard/ Visualization for OpenSearch	Mandatory	OpenSearch Dashboard visualizes and analyzes data for 5G NFs, offering interactive insights and custom reporting. **Impact**: Without visualization capabilities, understanding NF performance metrics and trends would be difficult, limiting informed decision-making.

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

Software	Tested Software Version			Software Requirement	Category	Sub-Category	Category Requirement	Usage Description
	NF 25.1.2xx	NF 25.1.1xx	NF 24.3.x					
AlertManager	0.28.0	0.27.0	0.27.0	Recommended	Alerting	Alerting (Integration with Prometheus)	Mandatory	Alertmanager is a component that works in conjunction with Prometheus to manage and dispatch alerts. It handles the routing and notification of alerts to various receivers. **Impact**: Not implementing alerting mechanisms can lead to delayed responses to critical issues, potentially resulting in service outages or degraded performance.
prometheus-kube-state-metric	2.15.0	2.13.0	2.13.0	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.

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

Software	Tested Software Version			Software Requirement	Category	Sub-Category	Category Requirement	Usage Description
	NF 25.1.2xx	NF 25.1.1xx	NF 24.3.x					
Prometheus Operator	0.80.1	0.76.0	0.76.0	Recommended	Monitoring	Prometheus Instance Management in Kubernetes	Conditional	The Prometheus Operator is used for managing Prometheus monitoring systems in Kubernetes. Prometheus Operator simplifies the configuration and management of Prometheus instances. **Impact**: Not using this operator could complicate the setup and management of monitoring solutions, increasing the risk of missed performance insights.
prometheus-node-exporter	1.8.2	1.8.2	1.8.2	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.
Prometheus	3.2.0	2.52	2.52	Mandatory	Monitoring	Metrics/ Monitoring System	Mandatory	Prometheus is a popular open-source monitoring and alerting toolkit. It collects and stores metrics from various sources and allows for alerting and querying. **Impact**: Not employing this monitoring solution could result in a lack of visibility into NF performance, making it difficult to troubleshoot issues and optimize resource usage.

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

Software	Tested Software Version			Software Requirement	Category	Sub-Category	Category Requirement	Usage Description
	NF 25.1.2xx	NF 25.1.1xx	NF 24.3.x					
Grafana	9.5.3	9.5.3	9.5.3	Recommended	Visualization	Monitoring/ Visualization Tool	Mandatory	Grafana is a popular open-source platform for monitoring and observability. It provides a user-friendly interface for creating and viewing dashboards based on various data sources. **Impact**: Without visualization tools, interpreting complex metrics and gaining insights into NF performance would be cumbersome, hindering effective management.
Calico	3.29.1	3.28.1	3.27.3	Recommended	Networking	Networking/ Network Security for Kubernetes	Mandatory	Calico provides networking and security for NFs in Kubernetes with scalable, policy-driven connectivity. **Impact**: CNI is mandatory for the functioning of 5G NFs. Without CNI and proper plugin, the network could face security vulnerabilities and inadequate traffic management, impacting the reliability of NF communications
metrics-server	0.7.2	0.7.2	0.7.1	Recommended	Monitoring	Resource Metrics for Kubernetes	Mandatory	Metrics server is used in Kubernetes for collecting resource usage data from pods and nodes. **Impact**: Without resource metrics, auto-scaling and resource optimization would be limited, potentially leading to resource contention or underutilization.

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

Software	Tested Software Version			Software Requirement	Category	Sub-Category	Category Requirement	Usage Description
	NF 25.1.2xx	NF 25.1.1xx	NF 24.3.x					
snmp-notifier	1.6.1	1.5.0	1.4.0	Recommended	Notification	SNMP Notification Service	Mandatory	snmp-notifier sends SNMP alerts for 5G NFs, providing real-time notifications for network events. **Impact**: Without SNMP notifications, proactive monitoring of NF health and performance could be compromised, delaying response to critical issues.
Jaeger	1.65.0	1.60.0	1.60.0	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	1.16.6	1.15.2	1.13.3	Recommended	Storage	Storage Orchestration	Mandatory	Rook is the Ceph orchestrator for Kubernetes that provides storage solutions. It is used in bm CNE solution. **Impact**: CSI is mandatory for the solution to work. Not utilizing Rook could increase the complexity of deploying and managing Ceph, making it difficult to scale storage solutions in a Kubernetes environment.

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

Software	Tested Software Version			Software Requirement	Category	Sub-Category	Category Requirement	Usage Description
	NF 25.1.2xx	NF 25.1.1xx	NF 24.3.x					
cinder-csi-plugin	1.32.0	1.31.1	1.30.0	Recommended	Storage	Block Storage Plugin	Mandatory	Cinder CSI (Container Storage Interface) plugin is for provisioning and managing block storage in Kubernetes. It is often used in OpenStack environments to provide persistent storage for containerized applications. **Impact**: Cinder CSI Plugin is used in OpenStack vCNE solution. Without this integration, provisioning block storage for NFs could be manual and inefficient, complicating storage management.

3.6 Security Certification Declaration

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

3.6.1 BSF Security Certification Declaration

Release 25.1.200

Table 3-6 BSF Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	Jun 30, 2025	No unmitigated critical or high findings
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	May 28, 2025	No unmitigated critical or high findings

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

Compliance Test Description	Test Completion Date	Summary
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	Jul 09, 2025	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	Jul 09, 2025	No findings

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

3.6.2 CNC Console Security Certification Declaration

Release 25.1.200

Table 3-7 CNC Console Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	Jul 09, 2025	No unmitigated critical or high findings
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	Jul 09, 2025	No unmitigated critical or high findings
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	Jul 09, 2025	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	Jul 09, 2025	No findings

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

3.6.3 OCCM Security Certification Declaration

Release 25.1.200

Table 3-8 OCCM Security Certification Declaration

Compliance Test Description	Test Completion	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	Jul 07, 2025	No unmitigated critical or high findings
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	Jul 07, 2025	No unmitigated critical or high findings

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

Compliance Test Description	Test Completion	Summary
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	Jul 07, 2025	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	Jul 07, 2025	No findings

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

3.6.4 OCI Adaptor Security Certification

Release 25.1.200

Table 3-9 OCI Adaptor Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	May 19, 2025	No unmitigated critical or high findings
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	NA	No unmitigated critical or high findings
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	Apr 28, 2025	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	Jul 08, 2025	No findings

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

3.6.5 NRF Security Certification Declaration

Release 25.1.200

Table 3-10 NRF Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	Jul 09, 2025	No unmitigated critical or high findings
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	Jul 09, 2025	No unmitigated critical or high findings
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	Jul 09, 2025	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	Jul 09, 2025	No findings

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

3.6.6 NSSF Security Certification Declaration

Release 25.1.200

Table 3-11 NSSF Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	Jul 02, 2025	No unmitigated critical or high findings
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	Jul 02, 2025	No unmitigated critical or high findings
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	Jul 02, 2025	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	Jul 02, 2025	No findings

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

3.6.7 Policy Security Certification Declaration

Policy 25.1.200

Table 3-12 Policy Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	Jul 01, 2025	No unmitigated critical or high findings
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	May 28, 2025	No unmitigated critical or high findings
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	Jul 09, 2025	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	Jul 09, 2025	No findings

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

3.6.8 SCP Security Certification Declaration

Release 25.1.201

Table 3-13 SCP Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	August 29, 2025	No unmitigated critical or high findings
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	August 29, 2025	No unmitigated critical or high findings
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	August 29, 2025	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	August 29, 2025	No findings

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

Release 25.1.200

Table 3-14 SCP Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	Jul 06, 2025	No unmitigated critical or high findings
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	Jul 06, 2025	No unmitigated critical or high findings
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	Jul 06, 2025	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	Jul 06, 2025	No findings

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

3.6.9 SEPP Security Certification Declaration

Release 25.1.201

Table 3-15 SEPP Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	Jul 17, 2025	No unmitigated critical or high findings. Scan done through Fortify.
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	Jul 04, 2025	No unmitigated critical, high, medium, and low findings. Scan done through RestFuzz.
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	Jul 17, 2025	No unmitigated critical or high findings. Scan done through Blackduck.
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	Jul 31, 2025	No issues found. Scan done through McAfee.

Release 25.1.200

Table 3-16 SEPP Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	Jul 08, 2025	No unmitigated critical or high findings. Scan done through Fortify.

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

Compliance Test Description	Test Completion Date	Summary
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	Jul 04, 2025	No unmitigated critical, high, medium, and low findings. Scan done through RestFuzz.
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	Jul 08, 2025	No unmitigated critical or high findings. Scan done through Blackduck.
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	Jul 08, 2025	No issues found. Scan done through McAfee.

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

3.6.10 UDR Security Certification Declaration

Release 25.1.200

Table 3-17 UDR Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	Jul 09, 2025	No unmitigated critical or high findings
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	Jul 09, 2025	No unmitigated critical or high findings
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	Jul 09, 2025	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	Jul 09, 2025	No findings

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

3.7 Documentation Pack

All documents for Oracle Communications Cloud Native Core (CNC) 3.25.1.2xx.0 are available for download on SecureSites and MOS.

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

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

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

4 Resolved and Known Bugs

This chapter lists the resolved and known bugs for Oracle Communications Cloud Native Core release 3.25.1.2xx.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 3.25.1.2xx.0.

4.2.1 BSF Resolved Bugs

Release 25.1.200

Table 4-1 BSF 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36715017	No health request going out from egress GW to scp as expected from MOP	The Egress Gateway experienced a critical failure in sending health requests to the SCP, impacting the system's ability to monitor its health status effectively. **Doc Impact:** There is no doc impact.	2	23.2.4
37390307	BSF generating SYSTEM_OPERATIONAL_STATE_NORMAL alert.	When the system operated in a normal state, the SYSTEM_OPERATIONAL_STATE_NORMAL alert was activated but failed to clear. This resulted in misleading alert notifications, as the system continued to indicate an alert state even when functioning normally. **Doc Impact:** Removed `SYSTEM_OPERATIONAL_STATE_NORMAL` alert from the "BSF Alerts" section in *Oracle Communications Cloud Native Core, Binding Support Function User Guide*.	3	24.2.1

Table 4-1 (Cont.) BSF 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37498738	Diam-gateway performing Reverse DNS lookup for unknown IPs	The diameter gateway was performing reverse DNS lookup for the unknown IP addresses. **Doc Impact:** There is no doc impact.	3	24.2.1
37392958	Parameter: podname missing from in BSF alert rules	The `podname` label was missing from the BSF alert rules. **Doc Impact:** There is no doc impact.	3	23.4.4
37512039	Audit services not running post mysqlmtd pods restart	When all the mysql data nodes goes down, audit-schedule records are lost. **Doc Impact:** There is no doc impact.	3	23.2.4
37553188	Signaling Connections' factor's value limit not upto the mark	The value limit assigned to the Signaling Connections factor was inadequate and required adjustment. **Doc Impact:** Updated the CNC Console configurations for NF scoring in the "NF Scoring Configurations" section of *Oracle Communications Cloud Native Core, Binding Support Function User Guide*.	3	23.4.2
36675490	BSF NetworkPolicy for nrf-client pod does not have proper label	The BSF NetworkPolicy for the nrf-client pod was missing the necessary labels, causing potential connectivity and security concerns. **Doc Impact:** There is no doc impact.	3	23.4.0

Table 4-1 (Cont.) BSF 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37815638	BSF - Missing step: during the NF user creation set BINLOG OFF	The steps to enable and disable BINLOG was missing in the installation guide. **Doc Impact:** Updated the BINLOG enable and disable procedure in the "Configuring Database, Creating Users, and Granting Permissions" section of *Oracle Communications Cloud Native Core, Binding Support Function Installation, Upgrade, and Fault Recovery Guide*.	4	24.2.2
38011392	BSF release document has missing database name	The overload management *ocbsf_overload* database was missing in the procedure for creating databases for Multisite deployment. **Doc Impact:** Updated the ocbsf_overload database details in the "Configuring Database, Creating Users, and Granting Permissions" section of *Oracle Communications Cloud Native Core, Binding Support Function Installation, Upgrade, and Fault Recovery Guide*.	4	25.1.100

Table 4-2 BSF ATS 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37404589	"BSFStaleSessionDetection_Phase2" feature failing	The BSFStaleSessionDetection feature was failing in the regression testing. **Doc Impact:** There is no doc impact.	3	23.4.5

Table 4-2 (Cont.) BSF ATS 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37820499	"BSF_SBI_Error_Codes " failing	The BSF_SBI_Error_Codes feature was failing in the regression testing. **Doc Impact:** There is no doc impact.	3	25.1.100

4.2.2 CNC Console Resolved Bugs

Release 25.1.200

Table 4-3 CNC Console 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37427171	PreProd: Policy CNCC 24.2.1 WARNINGS/ERRORS list of log messages	The public.dynamic.datamodel error/warning log messages were printed in cmservice pod logs. **Doc Impact:** There is no doc impact.	3	25.1.100
37899676	NF Selector not appearing in CNCC GUI	Occasionally, upon logging into the CNC Console Core, the NF instance selector dropdown fails to appear. This prevents users from accessing their desired NF Instance configuration. Instead, the cnPCF instance is displayed by default. **Doc Impact:** There is no doc impact.	3	24.2.1

Table 4-3 (Cont.) CNC Console 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38165407	Request to add check for golang version to CNCC Release Notes and Installation Guide	The CNC Console Installation, Upgrade, and Fault Recovery Guide needs to be updated with a note that informs the user that they must remove `ec_point_formats` from `clientDisabledExtensions` and `serverDisabledExtensions` to prevent deployment failure if they want to deploy CNC Console on a system with an older Kubernetes/Go version (for example, v1.23.10/go1.17.13). **Doc Impact:** Updated the note in the "Preupgrade Tasks" and "Customizing CNC Console" sections in *Oracle Communications, Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide.*	3	25.1.100

Note

Resolved bugs from 25.2.4 have been forward ported to Release 25.1.200.

4.2.3 cnDBTier Resolved Bugs

Release 25.1.201

Table 4-4 cnDBTier 25.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
38236749	Binlog cleanup command missing in example section of Restore DB procedure using local backup	While restoring ndb database, binlogs were not cleaned. The command `DELETE FROM replication_info.DBTIER_INITIAL_BINLOG_POSTION` was missing in the Restore procedure. **Doc impact**: Updated the sample output to include `DELETE FROM replication_info.DBTIER_INITIAL_BINLOG_POSTION` command in the "Downloading the Latest DB Backup Before Restoration" section in *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide.*	2	25.1.100
37864092	dbtscale_ndbmtd_pods script exited with 'Create Nodegroup FAILED' for wrong nodegroup	In a four site, ASM enabled, backup encrypted and password encrypted setup, the horizontal data pod scaling failed while using the dbtscale_ndbmtd_pods script and exited with 'Create Nodegroup FAILED" error. Wait for the new ndbmtd pods to start and assigned with the "no nodegroup" state before creating the node groups. **Doc Impact**: There is no doc impact.	2	24.2.5
38204318	Site removal script dbtremovesite is failing with error of script version mismatch on CNDB	While running the `dbtremovesite` site removal script, the script was failing due to the version mismatch. The cnDBTier library version was updated per the script version. **Doc impact:** There is no doc impact.	2	25.1.102

Table 4-4 (Cont.) cnDBTier 25.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
38204306	dbtremovesite script exits with ERROR - DBTIER_SCRIPT_VERSION (<25.1.100>) does not match DBTIER_LIBRARY_VERSION	Version of the `dbtremovesite` script did not match with the cnDBTier library version which resulted in an error. The cnDBTier library version was updated per the script version. **Doc impact**: There is no doc impact.	2	25.1.201
38224168	Update georeplication recovery procedure to remove duplicate steps	Updated the georeplication recovery procedure to remove the duplicated steps. **Doc impact**: Removed the steps that mention about the creation of NFs during georeplication failure recovery. For more information see the "Restoring Georeplication (GR) Failure" section in *Oracle Communications Cloud Native Core cnDBTier Installation, Upgrade, and Fault Recovery Guide*.	2	25.1.102
38200832	Schema change distribution is slowing down replication causing data discrepancy across 2 sites	In a multi-site Policy Control Function (PCF) setup, where site 1 (policy1) was completed a PCF application upgrade that included a schema upgrade, and site 2 (policy3) had fallen behind in replication, resulting in data discrepancies. **Doc impact**: There is no doc impact.	2	25.1.200
37668951	information_schema and table schema is seen to be inconsistent when policy upgrade was performed	After a policy upgrade, the metadata in information_schema did not reflect the actual table schema. **Doc impact**: There is no doc impact.	2	25.1.200
37978500	Incorrect key file for table 'SmPolicyAssociation'; try to repair it	The Incorrect key file for table error was encountered for specific tables like Smservice and common configuration tables. It is recommended to always reopen the table with the missing index. **Doc impact**: There is no doc impact.	2	23.4.6

Table 4-4 (Cont.) cnDBTier 25.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37975847	All data nodes experienced a simultaneous restart following the cnDBTier upgrade	A simultaneous restart of all data nodes (that is, all ndbmtd pods) following a cnDBTier upgrade was observed. **Doc impact**: There is no doc impact.	2	25.1.200
38278713	Document update required "DB Tier Stop Replica API" in User Guide	cnDBTier User Guide did not provide a reference in the "DBTier Stop Replica API" section to the procedure that explained the steps to gracefully start and stop georeplication between sites. **Doc impact** Added a reference to the "Stopping cnDBTier Georeplication Between Sites" section in the "DBTier Stop Replica API" section in *Oracle Communications Cloud Native Core cnDBTier User Guide*.	2	25.1.201
38220013	dbtrecover Script is affecting db-monitor-svc	A deadlock occurred in the db-monitor-svc during SQL pod restarts that caused connection assignment failure, as the monitoring service was unable to assign connections correctly. **Doc impact**: There is no doc impact.	3	25.1.100
38268348	Communication between db-monitor-svc and NF backend pods breaks during the ndbapp scaled down negative scenario	While implementing the following negative scenario in which a full traffic of SLF (50K lookup and 1.44K prov on site1), scaling the ndbapp pods from 7 to 0 for 15min. 2) after 15min again scaled up the ndbapp pods from 0 to 7. Fixed the deadlock in db-monitor-svc during SQL pod restart which caused connection assignment failure. **Doc impact**: There is no doc impact.	3	25.1.100

Table 4-4 (Cont.) cnDBTier 25.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37859265	dbtscale_ndbmtd_pods disrupted by ndbmtd pod restart	When dbtscale_ndbmtd_pods are run to scale data nodes (ndbmtd pods) on site1 from 8 to 14. The script was due to a ndbmtd pod restart during the scale operation is disrupted. **Doc impact**: There is no doc impact.	3	25.1.100
37859029	dbtscale_ndbmtd_pods failed when ndb backup triggered while scaling in progress	While scaling ndbmtd pods from 8 to 12 using the dbtscale_ndbmtd_pods script, thepods were scaled up, and REORGANIZE PARTITION had started. However, the script terminated with an error. **Doc impact**: There is no doc impact.	3	25.1.100
38129271	Upgrade from 23.4.0 to 25.1.100 broke replication between sites	Added the following new error numbers to the list of replication errors: • 1091 (Can't DROP – column/key doesn't exist) • 1826 (Duplicate foreign key constraint name) Removed the error "1094 - Unknown command" from the list. **Doc Impact**: There is no doc impact.	3	23.4.6
38144181	Add additional replication errors(1091, 1826) in the replication skip error section and remove 1094 replication erro from list	Added the following new error numbers to the list of replication errors: • 1091 (Can't DROP – column/key doesn't exist) • 1826 (Duplicate foreign key constraint name) Removed the error "1094 - Unknown command" from the list. **Doc impact**: There is no doc impact.	3	23.4.6

Table 4-4 (Cont.) cnDBTier 25.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37942052	dbtscale_ndbmtd_pods not working when release name contains prefix	When a single-site setup was deployed with a prefix used in the release name, and when the `dbtscale_ndbmtd_pods` script was run on this setup, the script was failing with the following error: "Error: UPGRADE FAILED: "mysql-cluster" has no deployed releases". This was because DBTIER_RELEASE_NAME was not set. **Doc impact**: There is no doc impact.	3	25.1.200
38197150	Horizontal data pod scaling failed using dbtscale_ndbmtd_pods script and exited with 'Create Nodegroup FAILED" error	In a four site, ASM enabled, backup encrypted and password encrypted setup, the horizontal data pod scaling failed while using the dbtscale_ndbmtd_pods script and exited with 'Create Nodegroup FAILED" error. Wait for the new ndbmtd pods to start and assigned with the "no nodegroup" state before creating the node groups. **Doc Impact**: There is no doc impact.	3	25.1.100
38288330	db-monitor-svc Requests Backup Transfer Status Before Transfer Starts	Georeplication recovery (non-fatal) was implemented using dbtrecover on a 2-site Georeplication (GR) setup with multi-channel replication with the following condition: • site 1 = Good site • site 2 = Site being recovered Errors were observed in the backup-mgr-svc pod on site-1 and no GRR related logs were printed in the backup-mgr-svc logs. **Doc Impact**: There is no doc impact.	3	25.1.200

Table 4-4 (Cont.) cnDBTier 25.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
38304684	Georeplication recovery failed with 6 channel replication channel over SM setup	Georeplication recovery was failing because the required Persistent Volume Claims (PVC) size for the replication service was not configured rightly. **Doc Impact**: There is no doc impact.	3	25.1.201
38314302	Document steps to create service account manually in case Helm MOP is enabled and individual flag are set as false with user defined name	cnDBTier documentation did not provide steps to create service account, roles, and role binding manually if user does not want automated service account creation. **Doc Impact**: Updated the steps to create the Namespace in the "Verifying and Creating Namespace" section. For more information, see *Oracle Communications Cloud Native Core cnDBTier Installation, Upgrade, and Fault Recovery Guide*		
38278476	Documentation for serviceAccounts/create flag is not clear when it is set as true	cnDBTier documentation did not provide comprehensive and clear documentation of RBAC configuration parameters. **Doc Impact**: Added a table "autoCreateResources Configurations" that provides autoCreateResources parameter configurations in different scenarios in the "LCM Based Automation" section in *Oracle Communications Cloud Native Core cnDBTier User Guide*		

Table 4-4 (Cont.) cnDBTier 25.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
38245044	Documentation should mention which site to be sourced in `dbtremovesite`	cnDBTier documentation did not provide details on which site must be used as the source when using the `dbtremovesite` script. **Doc Impact**: Updated the "Removing cnDBTier Cluster" section to specify which site must be used as the source when using `dbtremovesite` script. For more information, see *Oracle Communication Cloud Native Core, cnDBTier User Guide*.	4	25.1.200

> **Note**
>
> Resolved bugs from 25.1.103 and 24.2.6 have been forward ported to release 25.1.201.

Release 25.1.200

Table 4-5 cnDBTier 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37775811	Binlog cleanup command missing in example section of Restore DB procedure using local backup	While restoring ndb database, binlogs were not cleaned. The command `DELETE FROM replication_info.DBTIER_INITIAL_BINLOG_POSTION` was missing in the Restore procedure. **Doc impact**: Updated the sample output to include `DELETE FROM replication_info.DBTIER_INITIAL_BINLOG_POSTION` command in the "Downloading the Latest DB Backup Before Restoration" section in *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide.*	2	25.1.100

Table 4-5 (Cont.) cnDBTier 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37807135	dbtscale_ndbmtd_pods not working	The `dbtscale_ndbmtd_pods` script was failing in cnDBTier 24.2.5 single-site setup as the labels were not present in the stateful sets (STS). **Doc impact**: There is no doc impact.	2	24.2.5
37883263	dbtscale_vertical_pvc failing for ndbmgmd, ndbmysqld, ndbappmysqld, and ndbmtd	The dbtscale_vertical_pvc script contains a variable which can be configured for PVC size in the db-replication-svc deployment called "GEO_RECOVERY_RESOURCES_DISK_SIZE". However, this variable was not present in the db-replication-svc deployment in release 24.2.5. Hence, dbtscale_vertical_pvc script was failing for ndbmgmd, ndbmysqld, ndbappmysqld, and ndbmtd pods. **Doc impact**: There is no doc impact.	2	24.2.5
37978500	SQLException: Incorrect key file for table 'SmPolicyAssociation'; try to repair it	There was an incorrect key file for the table `Smservice`and common configuration tables, due to which Sm calls were failing. It is recommended to always reopen the table with the missing index. **Doc impact**: There is no doc impact.	2	23.4.6

Table 4-5 (Cont.) cnDBTier 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37864092	dbtscale_ndbmtd_pods script exited with 'Create Nodegroup FAILED' for wrong nodegroup	When the dbtscale_ndbmtd_pods script was run on a 4-site, ASM enabled, single channel cndBTier to scale the data pods, the script failed with the error, "Create Nodegroup FAILED" for wrong nodegroups. To clear the error, wait until the new ndbmtd pods to start and get assigned with the state "no nodegroup" before creating the node groups. **Doc impact**: There is no doc impact.	2	24.2.5
37859029	dbtscale_ndbmtd_pods failed when ndb backup triggered while scaling in progress	In a three site, multi-channel, cnDBTier setup while scaling of ndbmtd pods, the `dbtscale_ndbmtd_pods` script failed with the following error. "error 762 'Unable to alter table as backup is in progress'". **Doc impact**: There is no doc impact.	2	24.2.5

Table 4-5 (Cont.) cnDBTier 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release

37911174	Doc Changes: Stopping cnDBTier Georeplication Between Sites caused replication outage between all sites	While performing the steps given in the cnDBTier User Guide to stop the cnDBTier while performing georeplication between the sites, caused replication outage.
		Doc impact:
		Updated the following step in the "Starting or Stopping cnDBTier Georeplication Service" section:
		• Run the following command to stop the replication service switchover in cnDBTier with respect to siteName:
		`$ curl -X PUT http://$IP:$PORT/ocdbtier/georeplication/switchover/stop/sitename/{siteName}`
		For example, run the following command to stop the replication service switchover in cnDBTier with respect to cluster1:
		`$ curl -X PUT http://$IP:$PORT/ocdbtier/georeplication/switchover/stop/sitename/cluster1`
		Sample output:
		`{"replicationSwitchOver":"stop"}`
		For more information about how to start or stop cnDBTier Georeplication service, see *Oracle Communications Cloud Native Core cnDBTier Installation, Upgrade, and Fault Recovery Guide*.
			2	24.2.2

Table 4-5 (Cont.) cnDBTier 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37842445	dbtreplmgr uses hardcoded HTTP protocol causing failure in HTTPS-enabled setups	In a 4-site, HTTPS and TLS enabled, backup encryption and password encryption enabled setup, when the dbtreplmgr script was run to gracefully stop the replication, the replication did not stop and exited with an error. This was due to the script had a hardcoded HTTP parameter that caused the failure. **Doc impact**: There is no doc impact.	2	24.2.5
37076079	Data nodes are running on 99% disk usage	The Persistent Volume Claim(PVC) space for data node and SQL node were critically low and usage limit reached 99%. To monitor the PVC capacity, infra monitor container was injected to fetch the cnDBTier metrics from **db-replication-svc** service. **Doc impact**: There is no doc impact.	3	23.4.6
37859265	dbtscale_ndbmtd_pods disrupted by ndbmtd pod restart on 24.2.5	When the dbtscale_ndbmtd_pods script was run on a 4-site, ASM enabled, single channel cndBTier to scale the data pods, the script was disrupted by ndbtd pod restart. To resolve this, retried repartitioning the tables, if any data node was down or back up process was in progress. **Doc impact**: There is no doc impact.	3	24.2.5
36905360	CNDB-Upgrade:- ndbappmysqld-0 & ndbappmysqld-1 pods restart observed during CNDB upgrade	In a two-site Georeplication cnDBTier setup, pods were restarting during CNDB upgrade. By default, no-nodeid-checks parameter was set to enable for NDB pods. **Doc impact**: There is no doc impact.	3	24.2.0

Table 4-5 (Cont.) cnDBTier 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37466028	Event name should be displayed instead of eventtype = <integer value> in Cluster Events API	Each type of Cluster event was documented for better readability and understanding. **Doc impact**: Added a list of cluster event types that retrieve information about the events that occur in a cluster in the table "Cluster Event Types" in *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*.	3	25.1.100
37422096	Documentation is required to understand what does eventtype = <integer value> mean in API response	Each type of Cluster event was documented for better readability and understanding. **Doc impact**: Added a list of cluster event types that retrieve information about the events that occur in a cluster in the table "Cluster Event Types" in *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*.	3	25.1.100
37442733	Helm test is failing	The Helm test was failing as the `openssl`version was unknown during HTTPs certificate creation. **Doc impact**: Added a note that specifies the recommended version of `openssl`which is used to create certificates in the "Creating HTTPS or TLS Certificates for Encrypted Connection" section in *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*.	3	25.1.100

Table 4-5 (Cont.) cnDBTier 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37404406	Helm rollback from TLS to non-TLS same version not dropping TLS	While Upgrading or rolling back cnDBTier from a non-TLS to TLS enabled version, sites must be upgraded or rolled back twice. **Doc impact**: Added a note that explains how cnDBTier sites must be upgraded or rolled back twice while upgrading or rolling back cnDBTier clusters from a non-TLS version to TLS enabled version is added in the "Upgrading cnDBTier from Non-TLS to TLS Enabled Version (Replication)" section in *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*.	3	24.2.1
37672597	No response body in case of Retrieve all cluster Status Events API after restore is performed on setup	No response body in case of Retrieve all cluster Status Events API after restore is performed on setup. **Doc impact:** There is no doc impact.	3	25.1.100
37789389	dbtscale_vertical_pvc script doesn't work if ndbdisksize is in decimal	While installing a single site setup, when the value of the parameter `ndbdisksize` was set in decimal format, the `dbtscale_vertical_pvc` script failed. **Doc impact**: There is no doc impact.	3	25.1.100
37839960	ndbmtd pods always restart with initial option because of which the data nodes restart time will be increased when no MySQL NDB parameters is changed	`ndbmtd` pods always restarted with initial (--) option because of which the time taken to restart the data nodes increased even when MySQL NDB parameters were not changed. This was due to `cmp` command not found in the container. **Doc impact**: There is no doc impact.	3	25.1.100

Table 4-5 (Cont.) cnDBTier 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37753846	Vertical scaling of pvc failed using dbtscale_vertical_pvc script	The "dbtscale_vertical_pvc" script did not have an option to provide the name of the release due to which the script failed because the DBTIER_RELEASE_NAME was not set. **Doc impact**: There is no doc impact.	3	24.2.4
37855078	GRR is not working when the IPv6 address is configured in the remotesiteip configuration in db replication service deployment	If the db replication service deployment was configured with the IPv6 address in `remotesiteip`, the Georeplication Recovery (GRR) was not working. **Doc impact**: There is no doc impact.	3	25.1.100
37860493	dbtscale_ndbmtd_pods not working when release name contains prefix	When a single site setup was deployed with a prefix used in the release name, and when the `dbtscale_ndbmtd_pods` script was run on this setup, the script was failing with the following error: "Error: UPGRADE FAILED: "mysql-cluster" has no deployed releases". This was because DBTIER_RELEASE_NAME was not set. **Doc impact**: There is no doc impact.	3	24.2.5
37842199	Need a procedure for Ndbmtd recovery for continuous crashloop due to PVC corruption	The startup configuration must be updated in the NDB section of the custom value file. **Doc impact**: Updated the ndbmtd recovery procedure to add the startup configuration in the "Restoring Single Node Failure" section in *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*.	3	25.1.100

Table 4-5 (Cont.) cnDBTier 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37884064	Georeplication Recovery Status in CNCC needs to be changed from ACTIVE to NOT_RUNNING	During georeplication recovery (GRR) process, the status on the CNC Console displayed "ACTIVE" for both the sites, which was incorrect. The status on the CNC Console was updated to display "Not Active" or "Not Running" for such scenarios. **Doc impact**: There is no doc impact.	3	25.1.100
37952176	The metric db_tier_ndb_backup_in_progress temporarily shows a value of 1 when a data pod is deleted, even though no backup is actually running on the system	Even though no backup was running on the cnDBTier setup, when a data pod was deleted, the metric `db_tier_ndb_backup_in_progress` temporarily reports a value of 1. **Doc impact**: There is no doc impact.	3	25.1.100
37943375	The dbtscale_vertical_pvc script doesn't throw any error when wrong charts are provided to the script	The `dbtscale_vertical_pvc` script did not throw an error when wrong charts are provided to the script. The `dbtscale_vertical_pvc` script did not validate the chart version. **Doc impact**: There is no doc impact.	3	24.2.5
38161643	CNDBtier upgrade from 23.4.7 to 25.1.101 failed	cnDBTier upgrade from version 23.4.7 to version 25.1.101 (which was having Webscale version 1.3) was failing because the `kubectl exec` commands did not explicitly specify the container name in Pre/Post upgrade scripts. **Doc impact**: There is no doc impact.	3	25.1.100

Table 4-5 (Cont.) cnDBTier 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37902311	Rollback from TLS to Non-TLS still shows certificate in show replica status	The Upgrade and Rollback procedures did not specify that Updating the Non TLS to TLS and vice-versa procedures can disrupt the service. **Doc impact**: Added a note that specifies the downgrade procedure from TLS to Non-TLS is a disruptive procedure that may temporarily impact Geo-replication. Refer to the section "Rolling Back cnDBTier from Non-TLS to TLS Enabled Version (Replication)" in *Oracle Communication Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide.*	4	24.2.1
37399510	Support for Console Customized DBtier Custom Values File Parameters	The CNC Console parameter `global_max_binlog_size` was exposed in the `custom_values.yaml` file, by default. This parameter sets the size of the binary logs. **Doc impact**: Added the CNC Console parameter `global/api/max_binlog_size` parameter in the "Global Parameters" section in *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*.	4	25.1.100

Table 4-5 (Cont.) cnDBTier 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37343226	Implement the inclusive language practices and removing restricted terms from documents codes and logs	Implemented the inclusive language practices and removed restricted terms from documents, codes, and logs. **Doc impact**: Removed the restricted non-inclusive terms such as Slave, Master, Blacklist from the cnDBTier documentation set. See *Oracle Communications Cloud Native Core cnDBTier Installation, Upgrade, and Fault Recovery Guide* and *Oracle Communications Cloud Native Core, cnDBTier User Guide*.	4	24.3.0
37980727	Clarification Required for modifying the HTTPS/TLS secrets	The section "Certificates to Establish TLS Between Georeplication Sites" in cnDBTier Installation Guide for updating the secrets, did not specify to "Patch" the secret instead of recreating it when the certificate expires or when there is a change in the root CA. **Doc impact**: Updated the section "Certificates to Establish TLS Between Georeplication Sites" to patch the secrets instead of recreating them while establishing TLS between georeplication sites in *Oracle Communication Cloud Native Core, cnDBTier User Guide*.	4	24.2.1

Note

Resolved bugs from 25.1.101 and 24.2.5 have been forward ported to release 25.1.200.

4.2.4 CNE Resolved Bugs

Release 25.1.200

Table 4-6 CNE 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37799030	CNE images_25.1.100.tar missing Velero images	CNE 25.1.100 did not have the Velero images in the images tar file. This issue can lead to install and upgrade failures. **Doc impact**: There is no doc impact.	3	25.1.100
38204306	CNLB egress NAT is not working when there are two NFs on the same ServiceIpSet	Two NFs cannot communicate with each other via the external network, if they are in the same CNLB pair (ServiceIpSet), egress NAT is not performed.	3	24.3.1
37842711	CNE OpenStack installation failed due to `qcow` image changes	While Installing CNE 25.1.100 in Openstack (OL Image OL9U5_x86_64-kvm-b259) environment, `deploy.sh` script was failing with the ERROR `1: Bastion setup issue` error. **Doc impact**: There is no doc impact.	4	25.1.100

> **Note**
>
> Resolved bugs from 24.2.6, 24.3.3, and 25.1.101 have been forward ported to Release 25.1.200.

OSO Resolved Bugs

Release 25.1.200

There are no resolved bugs in this release.

4.2.5 NRF Resolved Bugs

Release 25.1.200

Table 4-7 NRF 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37839300	Secondary NRF(e1e2) sending 500 internal server errors towards SMSF when primary NRF w2 is taken OOR	When an NF switched from one NRF to another NRF, and if the NF Profile did not contain the `fqdn` attribute, the NRF processed the NF Profile successfully and saved it in the database. However, before generating the response, the NRF pegged the metric `ocnrf_nf_switch_over_total`, which indicated that the NF had switched over from one NRF to another. This metric had the dimension `NfFqdn`, which corresponded to the `fqdn` in the profile. Since the attribute was not present in the profile, the metric threw an exception and resulted in a Failure Response being generated. **Doc Impact:** There is no doc impact.	1	24.2.3

Table 4-7 (Cont.) NRF 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37912207	Feature Discovery Parameter Value Based Skip SLF Lookup backward compatible	Discovery queries using attributes other than `dnn` were not supported in `valueBasedSkipSlfLookupParams`. When the value-based Skip SLF feature was enabled, using query attributes other than `dnn` led to backward compatibility issues. Support was added to fall back to the older Skip SLF lookup mechanism when the value-based Skip SLF feature was enabled and the query attribute was not `dnn`. **Doc Impact:** There is no doc impact.	2	25.1.100
37912978	SLFOptions configuration not working after upgrade	The `SLFOptions` configuration did not work after the upgrade. The issue was caused by the upgrade logic related to the `SLFOptions` configuration. **Doc Impact:** There is no doc impact.	2	25.1.100
37788289	Discovery query results in Empty Profile when discovery query is forwarded due to AMF profile is Suspended and Empty response received from Forwarded NRF.	During NF profile processing, if a NF profile did not match the `guami` query parameter, NRF did not process the suspended profiles when the EmptyList feature was enabled for AMF. **Doc Impact:** There is no doc impact.	3	24.2.4

Table 4-7 (Cont.) NRF 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37784967	discovery response contains Profile having load value(30) greater then DiscoveryResultLoadThreshold (20)	If the `NFService` load was not present, the `NFProfile` load was not used to perform validation for the `DiscoveryResultLoadThreshold` feature. **Doc Impact**: There is no doc impact.	3	24.2.4
37704295	Discovery requests with preferred-locality return otherLocalityInd attribute as "false" despite non-matched localities.	Discovery requests from consumer NFs that included the `preferred-locality` parameter were returning the `otherLocalityInd` attribute as **"false"**, even when there were non-matching localities among the returned `NFProfiles`. The values of `otherLocalityInd` and `preferredLocalityMatchInd` were set based on both the preferred locations configured in the NRF and the locality attribute present in the discovery query. The values of `otherLocalityInd` and `preferredLocalityMatchInd` were set based **only** on the locality attribute in the discovery query. **Doc Impact:** There is no doc impact.	3	23.4.5

Table 4-7 (Cont.) NRF 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37135700	Delay Nnrf Services - Small Load Condition	NRF did not send `SETTINGS_MAX_CONCURRENT_STREAMS` in the HTTP/2 settings frame. As a result, the client considered the maximum number of concurrent streams to be 1, which caused requests to be queued and eventually time out. Consumers were not able to create concurrent streams to send traffic. NRF sent the `SETTINGS_MAX_CONCURRENT_STREAMS` based on the Helm configuration `serverDefaultSettingsMaxConcurrentStream`, which was set to 1000 by default in version 25.1.200. **Doc Impact:** There is no doc impact.	3	23.4.0

Table 4-7 (Cont.) NRF 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
36989541	The Number of concurrent HTTP2 streams is not limited	NRF did not send `SETTINGS_MAX_CONCURRENT_STREAMS` in the HTTP2 settings frame. Due to this, the client considered the concurrent stream as 1, which causes requests to be queued and times out. **Doc Impact:** This behavior is controlled by the `ingressgateway.serverDefaultSettingsMaxConcurrentStream` parameter. For more information, see "Ingress Gateway Microservice Parameters" in *Oracle Communications Cloud Native Core, Network Repository Function Installation, Upgrade, and Fault Recovery Guide.*	3	23.4.0

Table 4-7 (Cont.) NRF 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37187942	Incorrect Discovery Response when EmptyList and Forwarding feature enabled together for feature	When the emptyList and forwarding features were enabled, and NRF had profiles matching the target-nf-type in the REGISTERED and SUSPENDED states—but with only the SUSPENDED profiles matching the discovery query—these profiles were not considered while sending the discovery response. Due to this issue, even when there were profiles matching the discovery query in the SUSPENDED state and the emptyList feature was enabled, NRF sent back an empty discovery response. This scenario needed to be handled to send the matching SUSPENDED profiles as part of the emptyList response. **Doc Impact:** There is no doc impact.	3	24.3.0

Table 4-7 (Cont.) NRF 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
38026282	Response code from NRF is coming 400, instead of 500 when the backend services is down.	By default, NRF sent the incorrect error code 400 when the backend service was not available. The error code value was changed to 500 for *Unknown Host Exception* cases in the deployment YAML. Please find the updated configuration below: *name: ERR_UNKNOWN_HOST* *errorCode: 500* *errorCause: "Unknown Host Exception at IGW"* *errorTitle: "Unknown Host Exception"* *errorDescription: "Unknown Host Exception"* **Doc Impact**: There is no doc impact.	3	25..1.100

Table 4-7 (Cont.) NRF 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37760760	Incorrect ingress gateway port number was whitelisted in NRF network policy's allow-ingress-sbi section for https connections	An incorrect Ingress Gateway port number had been whitelisted in the NRF network policy's `allow-ingress-sbi` section for HTTPS connections. As a result, the NRF network policies did not function as expected, since HTTPS requests to the Ingress Gateway were blocked due to the incorrect port configuration. The NRF network policy custom values YAML was subsequently updated with the correct Ingress Gateway port number for HTTPS connections. The ports should have the values "8081" and "8443". **Doc Impact**: There is no doc impact.	3	24.2.3
35675295	NRF- Missing mandatory "iat claim" parameter validation is not happening in CCA header for feature - CCA Header Validation	NRF was not validating missing mandatory "iat claim" parameter in CCA header. **Doc Impact**: There is no doc impact.	3	23.2.0

Table 4-7 (Cont.) NRF 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37797310	NFRegistration logs some attributes are showing wrong data	The ThreadContext was not properly cleared after each request. In certain error scenarios, particularly when Input/Output errors occurred while reading the input message the controller method was never reached. As a result, values like nfInstanceID, requestUrl, and so on, were retained from previous requests due to context leakage. **Doc Impact**: There is no doc impact.	4	24.2.4
37417637	Disable/Hide CCA Header Validation Flag (which is not applicable for NRF use case) from NRF CNCC GUI	The "**enabled**" field under CCA Header screen in CNC Console GUI was editable (reason: the "readonly" flag for fields is configured to false by default). The "**enabled**" field flag is read-only now. **Doc Impact**: There is no doc impact.	4	24.2.2

Table 4-7 (Cont.) NRF 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
36707560	NRF Rest API "ALL_NF_TYPE" coming back even after deleting in the Discovery Validity Period table	The NRF REST API "ALL_NF_TYPE" reappeared even after it was deleted from the Discovery Validity Period table. On the CNC Console GUI, users observed that in **EDIT** mode, the **SAVE** operation was successful when **DELETE** was attempted to clear the list. However, after saving, the deleted row reappeared, resulting in no effective change. **Doc Impact**: There is no doc impact.	4	24.1.0
35672666	NRF- Incorrect "detail" value in CCA Header Response when missing mandatory "exp/aud claim" for feature - CCA Header Validation	NRF was sending an incorrect message in the `detail` attribute of the `ProblemDetails` field during CCA. **Doc Impact**: There is no doc impact.	4	23.2.0

Note

Resolved bugs from 24.2.4 have been forward ported to Release 25.1.200.

Table 4-8 NRF ATS 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37826579	NRF ATS installation is failing on clusters which do not have ASM installed.	NRF ATS installation failed on clusters which do not have ASM installed. The VirtualService resource did not have a flag to enable or disable its creation with respect to the ASM deployment. In clusters where ASM was not installed, the `VirtualService` CRD was not present, caused the ATS installation to fail. The `istio-vs.yaml` was placed under a flag to disable its creation in non-ASM deployments.	2	25.1.100

4.2.6 NSSF Resolved Bugs

Release 25.1.200

Table 4-9 NSSF 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38107817	NSSF 25.1.100 | NSSF Installation fails when readOnlyRootFilesystem is set to true	The NSSF 25.1.100 installation failed to complete on an OpenShift environment when the readOnlyRootFilesystem parameter was set to true in the YAML configuration. The nsauditor-pre-install pod encountered an error, and the logs revealed that the application was unable to start the web server due to a read-only file system. Specifically, the application was unable to create a temporary directory in /tmp. **Doc Impact**: There is no doc impact.	2	25.1.100
36889943	traffic moves from site2 to site1 , we are getting 404 error code for ns-availability scenarios	A 404 error code was encountered when traffic was moved from Site 2 to Site 1 in an ns-availability scenario within a 3 GR site deployment. Each site had 3.5 traffic, and the replication channel was functioning correctly. During the failover, traffic routing from Site 3 to Site 1 and Site 2 to Site 1 was initiated. **Doc Impact**: There is no doc impact.	3	24.2.0
37591102	OCNSSF:24.2.x:snmp MIB Complain from SNMP server	An issue was encountered with the OCNSSF 24.2.x version's SNMP MIB, where the SNMP server reported an error. The SNMP notifier was appending ".1" to the SNMP trap, causing a discrepancy. **Doc Impact**: There is no doc impact.	3	24.2.0

Table 4-9 (Cont.) NSSF 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37387621	NSSF DELETE method support for AMF Resolutions	The user requested the addition of support for the DELETE method in AMF Resolutions. The user expected that if an AMF resolution entry can be created manually, it should also be possible to delete it using the same interface. **Doc Impact**: There is no doc impact.	3	24.1.0
37773632	[10.5K TPS] when we are deleting all cnDBTier pods, ns-selection 2 pods have stuck in a 1/2 state.	When deleting all cnDBTier pods in a performance setup, two ns-selection pods became stuck in a 1/2 state, causing the replication channel to break. This issue occurred in a 3 GR Site setup with 10.5K TPS traffic on Site 1. **Doc Impact**: There is no doc impact.	3	25.1.100
37802321	helm upgrade for NSSF was stucked as hook failed to remove entry for previous release from common config table	The helm upgrade process for NSSF was stuck due to a failure in the post-install hook to remove the entry from the common configuration table. This issue occurred during the upgrade of Site-2. **Doc Impact**: There is no doc impact.	3	25.1.100
37474162	NSSF 24.3.0 - ConfiguredNssai must be present If Requested NSSAI includes an S-NSSAI not valid	NSSF's behavior deviated from the TS 29.531 standard for NS Selection service when the "Enhanced Computation of AllowedNSSAI" feature was disabled. According to the user guide, the NSSF should comply with the standard in such cases. **Doc Impact**: There is no doc impact.	3	24.3.0

Table 4-9 (Cont.) NSSF 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37681032	NSSF 24.2.1: Missing Edit Option for nsconfig Logging Levels in CNCC GUI	The "Edit" option for the nsconfig logging level was missing in the CNCC GUI of NSSF 24.2.1. Upon clicking the Logging Level Options, the REST API path /nssf/nf-common-component/v1/all/ logging returned all services, including nsconfig. However, when attempting to edit, the API path /nnssf-configuration/v1/cncc/ datamodel/conLoggingLevel did not include nsconfig in the list of services. **Doc Impact**: Updated the "Logging Level Options" section in *Oracle Communications Cloud Native Core, Network Slice Selection Function User Guide*.	3	24.2.1
37578617	OCNSSF[25.1.100: The behaviour of nnssf-nssaiavailability/v1/nssai-availability in case of update session data for unknown PLMNs not as per user guide	When updating session data for unknown PLMNs using the nnssf-nssaiavailability/v1/ nssai-availability endpoint in OCNSSF 25.1.100, the response received was "NOTAUTHORIZED" instead of the expected "PLMNNOT_SUPPORTED" as per the user guide. **Doc Impact**: There is no doc impact.	3	25.1.100
36844482	Alternate-route cache is not deleting the SCP entry after TTL(Time to live)	The alternate-route cache in NSSF 24.2.0 failed to delete SCP entries after their Time to Live (TTL) expired. This issue was observed during health checks and subsequent deregister requests. **Doc Impact**: There is no doc impact.	3	24.2.0

Table 4-9 (Cont.) NSSF 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36528105	3.5K TPS : 99.99% Failures seen when Rate-limiting feature is enabled in ASM setup	When the rate-limiting feature was enabled in an ASM setup with 3.5K TPS, the NSSF failed to handle 1 TPS requests, resulting in 99.99% failures. **Doc Impact**: There is no doc impact.	3	24.1.0
37776049	Dynamic log level updating Using CNCC for various micro services for NSSF. "LogDiscarding" Option is coming while fetching configured log level via REST but in CNCC while configured that option is not present	When updating log levels dynamically for various NSSF microservices using CNCC, the "LogDiscarding" option was present in the REST response but was not available in the CNCC configuration. This issue was observed specifically for the nssubscription and nsconfig microservices. **Doc Impact**: Updated section "Logging Level Options" in *Oracle Communications Cloud Native Core, Network Slice Selection Function User Guide*.	3	25.1.100
37136248	If dnsSrvEnabled is set to false and peer1 is used as a virtual host, the egress gateway will not sending the notification to peer2 host and peer health status is empty	When `dnsSrvEnabled` is set to **false** and peer1 is configured as a virtual host, the egress gateway failed to send notifications to peer2, resulting in an empty peer health status. **Doc Impact**: There is no doc impact.	3	24.2.1
37926363	NSSF Georedundancy - No Subscription sent to NRF after initial deployment	NSSF subscription failed to send to NRF post-deployment. Success required a pod restart. Logs revealed potential issues with allowedNfTypes and subscription handling. **Doc Impact**: There is no doc impact.	3	25.1.100

Table 4-9 (Cont.) NSSF 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37895878	NSSF 25.1.100 - Critical Pods in CrashLoopBackOff State in 3 Site GRR Setup	User encountered pod issues in a 3-site GRR environment due to database removal confusion during NSSF 25.1.100 installation. Clarification was needed on the correct database removal procedure for partial site uninstallation. **Doc Impact**: There is no doc impact.	3	25.1.100
37303227	[NSSF 24.3.0] [EGW-Oauth feature] "Oc-Access-Token-Request-Info:" IE should not come in notification.	In NSSF 24.3.0, when the EGW-Oauth feature is enabled, the "Oc-Access-Token-Request-Info" header was incorrectly included in the notification sent to the AMF. This issue was observed during a scenario where AMF subscribed to TAC and slice additions/deletions triggered notifications. **Doc Impact**: There is no doc impact.	4	24.3.0
37590706	NSSF is sending wrong response code when received patch remove request and authorizedNssaiAvailabilityData is empty	When NSSF received a PATCH remove request with an empty authorizedNssaiAvailabilityData, it sent an incorrect response code of 500 Internal Server Error instead of the expected 400 Bad Request. This issue was observed during a test scenario involving availability PUT and PATCH operations. **Doc Impact**: There is no doc impact.	4	25.1.100
38043793	NSSF ocnssf-custom-values-25.1.100.yaml does not expose containerPortNames	The 25.1.100 NSSF custom values YAML lacked the containerPortName, causing issues with CNLB annotations. To prevent misconfigurations, the containerPortName should be added to the YAML, aiding customers in setting up Multus-based traffic segregation. **Doc Impact**: There is no doc impact.	4	25.1.100

4.2.7 OCCM Resolved Bugs

Release 25.1.200

There are no resolved bugs in this release.

4.2.8 Policy Resolved Bugs

Table 4-10 Policy 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37197661	SOS Call is not working when subscriber is in KDDI PLMN	While processing CCR-U messages with UserLocationInfo, if the *GeographicLocationType* was set to 130, the system retained the MCC-MNC value of the TrackingAreaIdentifier but incorrectly handled the MCC-MNC of the EUTRANCellGlobalIdentifier. **Doc Impact:** There is no doc impact.	1	23.4.5
37470856	SOS call failure as Rx RAR is not initiated	PCF was not initiating Rx RAR which caused SOS call failures. **Doc Impact:** There is no doc impact.	1	23.4.7

Table 4-10 (Cont.) Policy 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37234674	SQLException on put	During the processing of RAR/ASR, if an AppSession was not found in the database due to race conditions or previous database errors, the action was canceled without performing any cleanup on the AppSessionInfo. This resulted in stale AppSessionInfos and associated PCC rules remaining active in the SmPolicyAssociation, causing the session to exceed the permitted size limit in the database. **Doc Impact:** There is no doc impact.	2	23.4.5

Table 4-10 (Cont.) Policy 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37372614	Post upgrade SM-PCF to 23.4.6 customer facing multiple errors	In the specified deployment, the virtualHost FQDN was configured to be resolved only for the HTTPS scheme, but the sbiRouting peerSetConfiguration was set to look up both HTTP and HTTPS. This discrepancy caused an issue when the Egress Gateway attempted to resolve the FQDN for HTTP, as it could not find any entry, resulting in an empty list. Consequently, while iterating over the list, the Egress Gateway encountered an exception, and the lookup for HTTPS was never initiated. **Doc Impact:** There is no doc impact.	2	23.4.4
37180729	SMPCF - Policy Evaluation Failure	The bug was caused by the configuration data cache in the Policy-blockly, which only accepted higher versions. As a result, when a snapshot with an older or lower version was taken, the cache failed to update. **Doc Impact:** There is no doc impact.	2	23.4.6

Table 4-10 (Cont.) Policy 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36927324	No error codes observed in the Egress GW Grafana dashboard when FQDN is mis-configured	After redirecting 1% of the traffic to the new site 002, the Egress Gateway pod logs displayed 500 internal errors due to a misconfigured SCP FQDN. But, no error codes related to this issue were observed in the Egress Gateway Grafana dashboard. If the FQDN had been incorrect, one would typically expect to see error codes like 502 or similar in the dashboard's graphs. **Doc Impact:** There is no doc impact.	2	23.4.4
36885688	Huge logs are flooding as "Exit requested from Policy evaluation" due to end all blockly	The EndAll blockly was logging action execution at the WARN level, resulting in a large number of messages displaying information about its execution. **Doc Impact:** There is no doc impact.	2	22.4.4

Table 4-10 (Cont.) Policy 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37469941	All nrf-client Discovery pods restarted due to out of memory	The database operations faced challenges due to concurrent updates by multiple NrfClient discovery pods. When attempting to modify NF profiles, the lack of a fixed update order and the acquisition of exclusive locks on different rows resulted in deadlocks and lock wait timeouts, impacting both read and write operations. **Doc Impact:** There is no doc impact.	2	23.4.4
37422360	5G Notification response failure on N7 due to space at end of flowDescription value.	During the SmRx call flow, when processing a specific Flow-Description value, the system incorrectly inserted a space after the keyword 'any' while reading the DiameterIPFilterRule. **Doc Impact:** There is no doc impact.	2	24.3.0

Table 4-10 (Cont.) Policy 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37435658	PCF respond Sy SNA with error code 5012 (Diameter_unable_to_comply)	The initial SLR-I/I response from the OCS lacked Policy Counters, causing the system to store a null value for existing Policy Counters. When the OCS later sent an SNR with Policy Counters, the null value triggered a Null Pointer Exception during processing, resulting in a 500 error and subsequently a 5012 response to the OCS. **Doc Impact:** There is no doc impact.	2	23.4.7
37841874	PCF 23.4.9 initiating incorrect Rx RAR causing SOS call failure || Event-trigger collision	If any fields related to event triggers were present in the CCR-U request, it was mistakenly interpreted as having both ACCESS_NETWORK_INFO_REPORT and/or RAN_NAS_Cause event triggers active. **Doc Impact:** There is no doc impact.	2	23.4.9

Table 4-10 (Cont.) Policy 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37616237	Multiple failures observed and KPI impact	An intermittent failure occurred during the SM-Service pod startup when establishing a connection to the database. Consequently, the SmPolicyAssociationDAO remained uninitialized, causing the pod to continue operating despite all attempts to interact with the SmPolicyAssociation table failing. **Doc Impact:** There is no doc impact.	2	23.4.4
37581343	Multiple PRE pods restarted in Sanda site	The existing process for CRUD operations on Managed Objects (MOs) was inefficient due to high memory consumption. When a CRUD operation was performed, the entire cache was transmitted to all worker nodes, resulting in unnecessary data transfer and resource utilization. **Doc Impact:** There is no doc impact.	2	23.4.7

Table 4-10 (Cont.) Policy 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37858170	metrics ocpm_udr_tracking_reponse_total_G is gradually increasing	The current counter creation process, triggered when a new datasource is added, generates counters for all combinations of tags. This results in an excessive number of counters, leading to increased memory consumption and unnecessary workload for the Java thread, as it has to manage and provide data for these counters. **Doc Impact:** There is no doc impact.	2	24.2.0
37796559	UDR w2 showing suspended in the PCF discovery even though it is registered fine at the NRF	When duplicate entries were encountered, the system correctly threw an exception indicating that a unique value was not returned, as it was designed to expect only one record. **Doc Impact:** There is no doc impact.	2	24.2.3

Table 4-10 (Cont.) Policy 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37777422	SM-PCF 003 Diam-connector Timeouts	The TCP connection for diam-conn experienced an issue where it stopped sending requests for approximately one hour. Upon investigation, it was discovered that the connection had exhausted all available streams, reaching the maximum limit of 2^32 - 1. **Doc Impact:** There is no doc impact.	2	23.4.6
37736253	Observed 500 Internal Error due to Audit Notifications	The system experienced a sequence of events that impacted its functionality. Initially, the EGW pods, starting before the ARS pods, faced challenges resolving the SCP FQDN, leading to message delays. Subsequently, the ARS lookup query returned a 503 response, suggesting temporary service overload or maintenance. **Doc Impact:** There is no doc impact.	2	23.4.4

Table 4-10 (Cont.) Policy 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37769150	Calls failing when calls made on HOLD	During a performance test, after restarting all Config Server and PRE pods, some PRE pods encountered an issue and failed to evaluate, despite the project being in the Production state. **Doc Impact:** There is no doc impact.	2	24.2.3
37725090	PCC Rule named "volte" is not being sent by cnPCRF	An unexpected behavior occurred during rule installation. The Volte rule, despite being sent for installation by PRE, did not successfully install in CCA. This was accompanied by a NULL pointer exception in the pcrf-core module when attempting to load PCC rules from the config-server. **Doc Impact:** There is no doc impact.	2	24.2.2

Table 4-10 (Cont.) Policy 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37693491	POD are taking high time to come UP during complete shutdown	When PRE functioned as a client, it established numerous new connections to the config-server, leading to excessive memory consumption and potential Out-Of-Memory (OOM) errors on the config-server. Additionally, this behavior caused the pods to experience prolonged startup times. **Doc Impact:** There is no doc impact.	2	24.2.2
37848496	sos failure while subscriber put normal Volte call on hold and dialed sos	The raceModerator's initial design could not detect race conditions when multiple rx/sd sessions were active for a single gxSession, as it only checked for session links in the registeredHandlers field. **Doc Impact:** There is no doc impact.	2	23.4.9

Table 4-10 (Cont.) Policy 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37830829	PCF not initiating Rx RAR causing SOS call failures	In high-performance scenarios, the system's event processing order was incorrect, leading to a sequence where NetLoc information was sent before the rxsession was stored, causing temporary unavailability. **Doc Impact:** There is no doc impact.	2	23.4.9
37830829	Observed LOW_MEMORY alert for nodeID 2	During an ongoing audit cycle, when the audit was disabled from the backend service and tables were requested to be deregistered from the audit, the system failed to update the AuditNotifyData to false. **Doc Impact:** There is no doc impact.	2	23.4.9
37070113	During rollback of PCF, nrf-dscovery pods get stuck in crashloopback state	The rollback of PCF can intermittently result in nrf-client discovery pods getting stuck in crashloopback state. This can lead to loss of egress traffic towards UDR in case of on demand discovery till the time rollback is successful. **Doc Impact:** There is no doc impact.	2	23.4.6

Table 4-10 (Cont.) Policy 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38107528	Policy 24.2.4 Different handling of UNKNOWN_RULE_NAME	During the processing of a CCR-U with an UNKNOWN_RULE_NAME for a predefined rule, the system mistakenly sent all other predefined rules from the session as Charging-Rule-Remove in CCA. **Doc Impact:** There is no doc impact.	2	24.2.4
37749812	Complete Shutdown did not get the PCF suspended || App-info not syncing	App-info prematurely exited its scraping loop, causing it to stop sending GET requests to cm-service for PCF's operational status updates. This led to App-info not reflecting the correct service status when PCF was partially or completely shut down. **Doc Impact:** There is no doc impact.	2	23.4.4

Table 4-10 (Cont.) Policy 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37043509	Observing "json.decoder.JSONDecodeError" in Performance pod of PCRF application	Concurrent read and write operations on the cgroup.json file caused data corruption. As one thread attempted to read while another was writing, the read thread accessed incomplete data, resulting in an invalid JSON format. This triggered a JSON.decoder error during the decoding process. **Doc Impact:** There is no doc impact.	3	23.4.0
37350850	Add a note in UG not to configure duplicate/same key name for traffic rule profiles	It was recommended to include a note in the User Guide advising against configuring duplicate or identical key names for traffic rule profiles to prevent potential issues. **Doc Impact:** A note is added in the Policy User Guide to avoid configuring duplicate or identical key names for traffic rule profiles. For more information, see *Oracle Communications Cloud Native Core, Policy User Guide*.	3	24.1.0

Table 4-10 (Cont.) Policy 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37390701	Policy generating SYSTEM_OPERATIONAL_STATE_NORMAL alert.	When the system operated in a normal state, the SYSTEM_OPERATIONAL_STATE_NORMAL alert was activated but failed to clear. This resulted in misleading alert notifications, as the system continued to indicate an alert state even when functioning normally. **Doc Impact:** Removed the SYSTEM_OPERATIONAL_STATE_NORMAL alert from the User Guide. For more information, see "List of Alerts" section in *Oracle Communications Cloud Native Core, Policy User Guide*.	3	24.2.1
37244455	Audit service not working with 2 Replicas	The presence of HTTP2 upgrade headers in the request from the audit service caused a "101 Switching Protocols" error when the binding service forwarded the request to pcrf-core, potentially resulting in missed stale contextBinding records. **Doc Impact:** There is no doc impact.	3	24.1.0

Table 4-10 (Cont.) Policy 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37208637	occnp_nrfclient_nf_status_with_nrf metric records as unknown from nrf-client-nfdiscovery pods	The occnp*nrfclient*nf*status*with_nrf metric showed conflicting values, indicating potential issues with its generation or reporting from the discovery pods. **Doc Impact:** There is no doc impact.	3	23.4.0
37213226	cnPCRF Rollover MK incorrect name	Usage-Mon currently enforces unique monitoring-key values for different plans, adhering to the 3GPP 29.512 standard. However, this poses a challenge for customers with legacy systems that allow the use of the same monitoring-key for multiple plans. **Doc Impact:** There is no doc impact.	3	23.4.0

Table 4-10 (Cont.) Policy 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37217249	Exporting diam-gateway congestion control	Parameters that are not configurable through the CNC Console are also not available for export through the same interface. For instance, the Diameter-Congestion-Control parameter is one such example. **Doc Impact:** Updated the export and import REST API details in the "Diameter Gateway Congestion Migration" section in *Oracle Communications Cloud Native Core, Policy REST Specification Guide*.	3	24.2.0
37220782	Alerts are not patching in Prometheus and Alert Manager	The alert file contained improperly indented YAML code, resulting in errors during its application. **Doc Impact:** There is no doc impact.	3 - Minimal Loss of Service	24.2.1

Table 4-10 (Cont.) Policy 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37220798	3GPP-SGSN-MCC-MNC AVP not sent to AF from PCF when in case of 5G	The system lacked support for the SGSNMCCMNC3 GPP AVP in AAA/STA messages, which was necessary when handling PLMN_CHANGE *requests from AAR.* Additionally, *the PLMN_CHANGE* dependency on PLMNInfo was overlooked, causing the system to incorrectly indicate that a supported feature was unavailable, which in turn impacted the handling of PLMN_CHANGE in 4G. **Doc Impact:** There is no doc impact.	3	23.4.0
37220798	Monitoring quota consume in a excess usage scenario - Granting Quota	The usage level value in umPolicyDecision unexpectedly turned negative in a create request following a terminate request, specifically when excess usage was enabled in the Data Limit Profile. **Doc Impact:** There is no doc impact.	3	24.2.1

Table 4-10 (Cont.) Policy 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37506006	Some Active Alerts not reflecting in NF Score Alert Section	The lack of namespace in generic alerts caused them to be omitted from the NF score, as the calculation relied on namespace-specific labels and expressions. **Doc Impact:** Added a note that NF score will calculate the alerts that contains namespace in the labels and expression in the "NF Scoring for a Site" section in *Oracle Communications Cloud Native Core, Policy User Guide*.	3	23.4.5
36744001	PCF status keeps fluctuating between REGISTERED and SUSPENDED state during complete shutdown	During a complete shutdown, the PCF status fluctuated between REGISTERED and SUSPENDED states instead of maintaining a consistent state. **Doc Impact:** There is no doc impact.	3	22.4.7
36669582	Policy Execution Logs missing when Policy has Syntax Error	If a syntax error was present in one sub-policy (such as P3) under a main policy, the logs reported the error in P3 but failed to include execution logs for the other sub-policies (P1 and P2). **Doc Impact:** There is no doc impact.	3	24.1.0

Table 4-10 (Cont.) Policy 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36589213	Issue updating Subscriber State Remote Variable	During Gx CCR-U processing, PCRF-Core project-specific variables were overridden by Usage-Monitoring (UM) variables. As a result, only the state variables from UM were sent to the PDS, while the PCRF-Core variables were not included. **Doc Impact:** There is no doc impact.	3	23.4.2
36821295	Subscriber trace of Policy Execution logging and "End All" block logging issue	The EndAll Blockly did not log action executions when used within a sub-policy. Logs were only added to the POLICY-EXECUTION SAL when the EndAll Blockly was used directly in the main policy. **Doc Impact:** There is no doc impact.	3	23.4.3
37096732	Exporting diam-gateway congestion control	Following an upgrade to release 24.1.0, the congestion control export functionality in the diam-gateway was found to support only Binding and Bulwark services. The option was not available for other services during bulk export. **Doc Impact:** There is no doc impact.	3	24.1.0

Table 4-10 (Cont.) Policy 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37236677	Timeout exception occurred while sending notification request to Notification Server	During HTTP/1.1 connection closure or server restart, the cleanup logic misidentified the connection as HTTP/2, causing a `ClassCastException`. This led to incomplete cleanup, preventing the connection count from reducing. As a result, new connections were blocked, causing pending requests to time out in the queue. **Doc Impact:** There is no doc impact.	3	23.2.0
37311210	VoNR Call failure - 503 service unavailable	On the SmRx call flow with the ACCESS_TYPE_CHANGE AfEvent, when the ratType in the AAA/RAR message was not one of the supported values (NR, EUTRA, WLAN, or VIRTUAL), the diam-connector failed to translate the message. This resulted in 5012 AAA responses or 500 RAA responses being triggered. **Doc Impact:** There is no doc impact.	3	23.4.4

Table 4-10 (Cont.) Policy 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37235770	CHIO cnPCRF, POD restarted chio-cnp-cnpcrf-notifier	Unbounded dimension values in metrics consumed excessive memory, leading to pod reboots. **Doc Impact:** There is no doc impact.	3	23.2.8
37940165	PCF Audit Schedules Rest API is not working	There were a few issues in Audit Scheduled REST API commands. **Doc Impact:** Updated the REST API commands for Audit Service in the "Audit service" section in *Oracle Communications Cloud Native Core, Policy REST Specification Guide*.	3	24.2.4
37033338	occnp_nrfclient_nf_status_with_nrf metric records as unknown from nrf-client-nfdiscovery pods	The `occnp_nrfclient_nf_status_with_nrf` metric from discovery pods reported `4/UNKNOWN`, contradicting the defined status values (0-4). Either these pods should not generate the metric or their values are incorrect. **Doc Impact:** There is no doc impact.	3 - Minimal Loss of Service	23.4.0

Table 4-10 (Cont.) Policy 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37315990	Policy UG Table 9-396 occnp_policy_processing_latency_ms has unrelated note	An unrelated note was added in the Policy User Guide for the `occnp_policy_processing_latency_ms` metric. This note did not pertain to the metric's actual functionality or context. **Doc Impact:** Removed the note which was not pertaining to `occnp_policy_processing_latency_ms` metric from the "PRE Metric" section in *Oracle Communications Cloud Native Core, Policy User Guide*.	3	24.2.0
37240047	Observing JVM heap memory usage alerts for multiple PCRF Core pods	Multiple PCRF core pods triggered `jvmHeapMemoryUsedBytes` alerts, showing memory usage up to 90-92%. This issue was noted on a DR site without any traffic, suggesting an unexplained increase in memory usage. **Doc Impact:** There is no doc impact.	3	23.4.5
37279607	cnPCRF CHIO, old sessions are not deleted by audit process in both sides CHIO & INDE	There were a few inconsistencies found between the cnPCRF CHIO and INDE systems. **Doc Impact:** There is no doc impact.	3	23.2.8

Table 4-10 (Cont.) Policy 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37219275	Metrics for discarded messages from Overload	the metrics `diam_overload_message_reject_total` and `diam_congestion_message_reject_total` were prefixed with `occnp_`, becoming `occnp_diam_overload_message_reject_total` and `occnp_diam_congestion_message_reject_total`. The User Guide was not updated to reflect this change, still listing the metrics without the `occnp_` prefix. **Doc Impact:** Updated a few diameter gateway metrics with *OCCNP* prefix in the "Diameter Gateway Metrics" section in *Oracle Communications Cloud Native Core, Policy User Guide*.	3	24.1.0
37446539	SESSION_LEVEL quota is allocated even though the base data limit profile is PCC_Level	When the base data limit profile was set to `PCC_Level`, a `SESSION_LEVEL` quota was allocated instead of a `PCC_LEVEL` quota. This occurred because the UMLevel was determined from the `umData` rather than from the base data limit profile, resulting in incorrect quota allocation. **Doc Impact:** There is no doc impact.	3	25.1.200

Table 4-10 (Cont.) Policy 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37440999	PCF Undeploy/ delete failed with Error	The PCF undeploy workflow failed and returned an error during execution. **Doc Impact:** There is no doc impact.	3	24.2.2
37467761	Policy export window is blank with export option disable	The Policy Project Import API permitted duplicate projects to be imported when no existing projects were present. This resulted in the Policy Export dialog appearing blank in the user interface. **Doc Impact:** There is no doc impact.	3	24.2.2
37607291	Diameter DWR timer modification procedure	Modifying the default 6-second Device Watchdog Request (DWR) interval in PCF responder connections via the Configuration Management UI and restarting Diam-GW pods had no effect, as DWRs continued at the original 6-second (±2 seconds) interval. **Doc Impact:** There is no doc impact.	3	24.2.2

Table 4-10 (Cont.) Policy 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37607744	PCRF Core getting 404 errors from PDS	There was no option to exclude PDS communication specifically related to SSV. Exclusion could only be applied based on user data types (for example, `smPolicyData`, `ldapData`) or all communication in general. **Doc Impact:** There is no doc impact.	3	24.2.2
37536314	Ingress gateway is flooded with overload disable feature logs (25.1.200)	Disabling SBI overload control in the CM GUI did not prevent `failure_count` and `pending_count` requests from being sent to Ingress_GW, as the `overloadManager` flag remained enabled by default in the perf-info deployment. **Doc Impact:** There is no doc impact.	3	24.2.2

Table 4-10 (Cont.) Policy 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37556610	5G Volte call failing due to incorrect "packetFilterUsage" value in SMF notify	The configuration parameter `setPacketFilterUsageToTrueForPreliminaryServiceInfo`, part of the `pcf.smservice.cfg` topic, was not properly read or applied in the code. As a result, despite being set to **false** in the GUI, it was internally set to **true** due to its default value in the code. **Doc Impact:** There is no doc impact.	3	23.4.7
37547046	observed to have AMF-PCF and UE-PCF failures	The UE service failed to send the `3gpp-sbi-callback` header in Update Notify requests to the AMF, causing the SCP to trim the callback URI and return a `500 INTERNAL_SERVER_ERROR`, even though the callback header was enabled in the GUI. **Doc Impact:** There is no doc impact.	3	23.4.4
37561938	Inconsistent 3gpp-sbi-correlation-info header	The `3gpp-sbi-correlation-info` header was received in an incorrect format, as a List instead of a String. **Doc Impact:** There is no doc impact.	3	24.2.2

Table 4-10 (Cont.) Policy 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37841874	Unable see the Audit Scheduled Data in Audit Service : Observing 404 Not Found	Audit-schedule records were lost when MySQL data nodes or the specific data containing them became unavailable, as the audit service only generated these records during service registration or audit-pod startup and did not regenerate them afterward. **Doc Impact:** There is no doc impact.	3	23.4.3
37453297	Policy CNCC 24.2.1 WARNINGS/ERRORS list of log messages	The topic `public.dynamic.datamodel` displayed an error or warning message when the `cmservice` was started. **Doc Impact:** There is no doc impact.	3	24.2.1
37444201	500 INTERNAL_SERVER_ERROR are reporting as INFO and not ERROR within the diam-connector	`500 INTERNAL_SERVER_ERROR` responses were logged as `INFO` instead of `ERROR` within the diam-connector. Ideally, 5xx errors should be reported under the `ERROR` log level rather than `INFO`. **Doc Impact:** There is no doc impact.	3	24.1.1

Table 4-10 (Cont.) Policy 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37201588	AMF_NFSetid_ODD_Caching_Global_Interface_Enabled Scenario failure	In the Regression feature, the scenario "AMF_NFSetid_ODD_Caching_Global_Interface_Enabled" within the `Non_SUPI_ODD_Caching_AM` test failed at the step validating the metric `occnp_nrfclient_discovery_cache_support_cache_hit_total`. The expected value was 1, but the actual value was 2, causing the test to fail. **Doc Impact:** There is no doc impact.	3	24.2.1
37416624	PCF 24.2.2: Overload control generates error	JSON decode errors occurred in the app-info pod logs when accessing the `service_monitor_status.json` file. This issue was caused by a race condition during concurrent read and write operations. **Doc Impact:** There is no doc impact.	3	24.2.2

Table 4-10 (Cont.) Policy 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37762694	Scaling Down of Pods During Shutdown & Bringing System Backup	When the diam-gateway (EGW) was scaled down for an extended period, the PCF audit microservice was not shut down, leading to potential deletion of audit records due to errors during auditing. Engineering recommended shutting down the audit microservice if Egress Gateway is down for hours or days and scaling it out before restoring normal operations. **Doc Impact:** Added a procedure for Scaling Down of Pods During Shutdown and Restoring System Backup in the "Uninstalling Policy" section in *Oracle Communications Cloud Native Core, Policy Installation, Upgrade, and Fault Recovery Guide*.	3	24.2.2

Table 4-10 (Cont.) Policy 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37731509	occnp_oc_egressgateway_peer_health_status reports incorrect peer health from one pod	The `occnp_oc_egressgateway_peer_health_status` metric reported peer health status only from the leader pod in PCF, excluding the secondary pod. This occurred because peer health pings were executed exclusively on the leader pod, causing the metric to show pegged values only for the leader. **Doc Impact:** There is no doc impact.	3	23.4.3
37726105	Incorrect log level for successful session audit attempt (RAR)	When the result code `DIAMETER_SUCCESS (2001)` was returned, it was logged at the `WARN` level in the diam-connector logs. However, successful result codes should be logged at the `INFO` level, as only non-successful codes warrant a `WARN` level. This resulted in hundreds of thousands of irrelevant `WARN` messages being logged daily. **Doc Impact:** There is no doc impact.	3	24.2.2

Table 4-10 (Cont.) Policy 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37835639	PCF populates 3gpp-target-api-root with port in 0 in n28 delete	PCF sent a DELETE request to CHF with port `0` when the location header from CHF did not include a port. Despite CHF successfully processing the request, PCF should have used the default port `80` when no port was specified in the location header. **Doc Impact:** There is no doc impact.	3	24.2.2
37767801	Policy Design documnet is not having any information about Try-Catch Blockly	The Try-Catch Blockly in the Logic section of the Policy Design document was not accompanied by an explanation or use case example. **Doc Impact:** Added the details for Try-Catch Blockly in the "Logic Category" section in *Oracle Communications Cloud Native Core, Policy Design Guide*.	3	24.2.4

Table 4-10 (Cont.) Policy 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36566264	Procedure to Enable/Disable Ingress and Egress Services	The customer sought to disable the ingress and egress services in the PCF NF during deployment for voice 4G-only use. Despite setting `ingress-gateway.enabled` to `false` in the custom YAML file, the ingress service remained active. The customer required a solution to disable these services during installation without post-deployment pod scaling. **Doc Impact:** Removed the ingress-gateway: enabled: false and egress-gateway:enabled: false configurations in *Oracle Communications Cloud Native Core, Policy Installation, Upgrade, and Fault Recovery Guide*.	3	23.1.0
36397776	PCF Install Failed on Post Upgrade - cm-service	Changing the `servicePort` to `8080` caused the post-install hook of the Configuration Management (CM) service to fail, resulting in a failed installation. **Doc Impact:** There is no doc impact.	3	23.4.0

Table 4-10 (Cont.) Policy 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37839791	Sy's SNR is not triggering RAR	Session Notification Requests (SNRs) failed to trigger policy evaluation, and no Re-Authorization Request (RAR) was issued. The Policy Data Store (PDS) indicated that the GPSI (preferred search index) was missing from the request. Despite a similar issue being addressed in bug 36290600 and fixed in version 23.2.8, the problem remained in version 24.2.2, suggesting the fix was not fully ported or the scenario was not entirely resolved. **Doc Impact:** There is no doc impact.	3	24.2.2
37578299	Observing high memory utilization in diameter gateway	To optimize memory management, the high-memory threshold for direct memory was set to 90% and made configurable via `values.yaml`. TCP send/receive buffer settings were introduced to avoid unnecessary memory consumption when the infrastructure defaulted to higher values. The default RAM usage was also raised from 25% to 40%. **Doc Impact:** There is no doc impact.	3	24.2.2

Table 4-10 (Cont.) Policy 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37061051	STR is not sent by PCF if CCA-I sent with error code	When a CCR-Initial (CCR-I) request was rejected or released by the Policy and Charging Rules Function (PCRF), the Policy Data Store (PDS) unsubscribe request was not sent to clean up the PDS GET operation that had occurred earlier. **Doc Impact:** There is no doc impact.	4	23.4.5
37458503	Update "lastresetTime" field on CNPCRF User-Guide	The `lastresettime` field in the CNCPRF User Guide was undocumented. It records the last reset time associated with a billing day change. In the absence of a billing day change, the `lastresettime` value is identical to the `resettime` field. **Doc Impact:** Added details for `lastresetTime` field in the "Usage Monitoring on Gx Interface" section in *Oracle Communications Cloud Native Core, Policy User Guide*.	4	23.4.3

Table 4-10 (Cont.) Policy 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36858008	BSF deregistration count came to zero after upgrading PCF to v23.4.3	After upgrading the PCF application and database, binding deregistration did not occur, and the count remained at zero. Additionally, BSF deletes were not being sent to the PCF application following the upgrade. **Doc Impact:** There is no doc impact.	4	23.4.3
36971270	QOS parameter : Max DataBurstVol" is taking values between 1-4065 and not 0 or null	The parameter "Max DataBurstVol" accepted values only between 1 and 4065, excluding 0 or null, which was a requirement. In earlier releases, such as 23.4.0, setting this parameter to 0 was possible. It is unclear whether this change in behavior is a bug or a design modification. **Doc Impact:** There is no doc impact.	4	24.1.0

Note

Resolved bugs from 24.2.6 have been forward ported to Release 25.1.200.

Table 4-11 Policy ATS 24.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37308415	Unexpected ServiceAccount Creation of ATS	Unexpected ServiceAccounts were created in ATS. **Doc Impact:** There is no doc impact.	3	24.3.0

Table 4-11 (Cont.) Policy ATS 24.3.0 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37307977	SM_PCF_as_producer_400 Scenario failure in Full NewFeatures	Under the New Features list, SM PCF as a producer feature failed with *400 bad requests* error. **Doc Impact:** There is no doc impact.	3	24.3.0
37283931	SM_Policy_Release_Session_Without_Cause Scenario failure in Regression	SM_Policy_Release_Session regression feature failed at the SM_Policy_Release_Session_Without_Cause scenario. **Doc Impact:** There is no doc impact.	3	24.2.2
37224604	NRF_Error_Response_Enhancement_PCF_as_Producer failure in NewFeature	Under the New Features list, NRF_Error_Response_Enhancement_PCF_as_Producer feature failed at NRF_UDR_Register_and_Suspension scenario. **Doc Impact:** There is no doc impact.	3	24.2.1
37305493	Bulwark_Support_SM_Create_Delete_Update Notify_PDSNotification_RedCap_ocLog failing	In the full regression pipeline, Bulwark_Support_SM_Create_Delete_Update Notify_PDSNotification_RedCap_ocLog feature failed in the initial run, but succeeded when the feature was rerun. **Doc Impact:** There is no doc impact.	3	24.2.1

Note

Resolved bugs from 24.2.6 have been forward ported to Release 25.1.200.

4.2.9 SCP Resolved Bugs

Release 25.1.201

Table 4-12 SCP 25.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38284085	SCP 25.1.200 Notification throwing NF_RULE_PROCESSOR_FAILURE for all NFs except UDR	While testing SCP 25.1.200, it was observed that routing rules for four test UDR profiles were processed and updated successfully. However, all other NF profiles were rejected, resulting in the following exception: "message":"Category: NF_RULE_PROCESSOR_FAILURE, Event: RULE_PROCESSOR_MISCELLANEOUS, EventId: OSCP-NTF-RULPRC-EV001" **Doc Impact**: There is no doc impact.	2	25.1.200
38206028	Error while trying to Upgrade SCP from 25.1.100 to 25.1.200 and on fresh install of 25.1.200	The following error was observed while upgrading SCP from 25.1.100 to 25.1.200: INSTALLATION FAILED: YAML parse error on ocscp/charts/scpc-configuration/templates/configuration.yaml: error converting helm.go:84: [debug] error converting YAML to JSON: yaml: line 19: did not find expected key YAML parse error on ocscp/charts/scpc-configuration/templates/configuration.yaml **Doc Impact**: There is no doc impact.	3	25.1.200
38318190	SCP 25.1.200 ModelD AUSF discovery failure: getAusfInfo() is null	During service discovery of the nausf-auth service for NRF, the AUSF profile was sent by NRF in the response. However, SCP encountered a 500 error because the Ausfinfo header was missing from the response. **Doc Impact**: There is no doc impact.	3	25.1.200

Table 4-13 SCP ATS 25.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38328447	Metric "ocscp_metric_nf_lci_tx_total" at times does not get validated if scp is not enabled to decode consumer on the basis of XFCC header and response from producer having LCI gets conveyed to Consumer NF	The ocscp_metric_nf_lci_tx_total metric was not consistently validated when SCP was not enabled to decode the consumer based on the XFCC header. As a result, responses from the producer NF containing LCI were incorrectly conveyed to the consumer NF. **Doc Impact**: There is no doc impact.	3	25.2.100

Release 25.1.200

Table 4-14 SCP 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37838652	SCP unable to send requests when maxStreamId is reached on a connection	SCP was unable to send requests when the stream ID reached its maximum value. **Doc Impact**: There is no doc impact.	2	25.1.100
37942341	SCP is erroneously routing inter-SCP traffic to other SCP instances within the same region.	SCP generated inter-SCP routing rules for instances that were located within the same region. **Doc Impact**: There is no doc impact.	2	25.1.100
38120012	SCP internal traffic sent to OCNADD despite fix for BUG 37226666 delivered in 24.2.2	The internal traffic from SCP 24.2.4 was incorrectly routed to OCNADD, even though a fix for this issue was provided in SCP 24.2.2. **Doc Impact**: There is no doc impact.	3	24.2.2
38012554	SCP/ ATS_25.1.100_Full_Regression_Failure_0252925	In SCP-ATS 25.1.100, a complete regression test failed with error codes. **Doc Impact**: There is no doc impact.	3	25.1.100
37931177	Notifications {"title":"Loop Detected","status":508" }	In SCP 25.1.100, notifications with the title "Loop Detected" and status code 508 were incorrectly generated. **Doc Impact**: There is no doc impact.	3	25.1.100

Table 4-14 (Cont.) SCP 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37859976	SCP is showing 504 errors for peer SCPs in the egress response metrics which excludes ocscp-initiated messages	SCP generated 504 errors when the peer SCP was unreachable and the destination route was exhausted. **Doc Impact**: There is no doc impact.	3	25.1.100
37843293	SCPMediationConnectivityFailure alerts are active even the connectivity is fine toward mediation	SCPMediationConnectivityFailure alerts were previously active despite confirmed connectivity toward Mediation. **Doc Impact**: There is no doc impact.	3	24.2.2
37840642	'DBOperation Failed: Failed to get ServiceEntry' exception was observed on the notification pod within the SCP	During a traffic run at the rate of 730K MPS with 700 NF profiles, a 'DBOperation failed to get service entry' exception occurred on the SCP. The setup included 7 SCP triplets in each region. **Doc Impact**: There is no doc impact.	3	25.1.100
37840553	A warning concerning an 'empty version map' was observed while running traffic at a rate of 730K MPS using a 700 NF profile.	While running traffic at a rate of 730K MPS using 700 NF profiles, a warning about an "empty version map" was observed. **Doc Impact**: There is no doc impact.	3	25.1.100
37815522	SCP Provides Grafana wrong Metric in Prometheus CPU utilization and Prometheus memory utilization	SCP provided incorrect metrics to Grafana for Prometheus CPU utilization and Prometheus memory utilization. **Doc Impact**: There is no doc impact.	3	24.2.2
37775369	SCPProducerNfSetUnhealthy Alert not getting raised	The `SCPProducerNfSetUnhealthy` alert was not raised. **Doc Impact**: There is no doc impact.	3	25.1.100
37746963	SCP Worker pod generating high Kube API traffic	In SCP 24.2.2, the SCP-Worker pod generated high Kubernetes API traffic. **Doc Impact**: There is no doc impact.	3	24.2.2

Table 4-14 (Cont.) SCP 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37721950	Getting IP instead of FQDN in peerscpfqdn dimension of SCPUnhealthyPeerSCPDetected Alert	The `peerscpfqdn` dimension of the `SCPUnhealthyPeerSCPDetected` alert displayed an IP address instead of FQDN. **Doc Impact**: There is no doc impact.	3	25.1.100
37721565	If SCP received request message with 3gpp-Sbi-Client-Credentials header with x5u - X.509 URL, then SCP should passthrough without CCA validation and should not reject the request message.	When SCP received a request message containing the 3gpp-Sbi-Client-Credentials header with an x5u (X.509 URL), it incorrectly rejected the message instead of bypassing CCA validation and processing the request. **Doc Impact**: There is no doc impact.	3	25.1.100
37713112	LCI and OCI not having validation for timestamp header causing nullPointerException leading to failure in responding to the consumer	LCI and OCI lacked validation for the timestamp header, which resulted in `NullPointerException`. This issue caused failures in responding to consumer NFs. **Doc Impact**: There is no doc impact.	3	25.1.100
37700589	SCP Notification pod restarted while sending invalid notification requests at a higher rate around 2K TPS	The SCP-Notification pod restarted when sending invalid notification requests at a high rate, approximately 2K TPS. **Doc Impact**: There is no doc impact.	3	25.1.100
37693288	SCP does not make NF rule profile for the de-registered NF on Last NF De-registration	SCP did not make NF rule profile for the de-registered NF on the last NF de-registration. **Doc Impact**: There is no doc impact.	3	24.3.0
37657153	Configuration pod crash was noticed on SCP when traffic was flowing at 730K MPS (signaling) and 1K TPS (control plane) GET requests to retrieve the ingress rate limit configuration	The configuration pod restarted in SCP when handling traffic at 730K MPS (signaling) and 1K TPS (control plane). This occurred during GET requests to retrieve the ingress rate limit configuration. **Doc Impact**: There is no doc impact.	3	25.1.100

Table 4-14 (Cont.) SCP 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37640874	SCP Metrics and dimensioning questions	Discrepancies related to metric dimensions and descriptions were observed in SCP 24.3.0. **Doc impact**: Updated the descriptions of the `ocscp_nf_end_point` dimension and the `ocscp_nrf_notifications_requests_nf_total` metric in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.	3	24.3.0
37640288	SCP Possibility to create subscriptions using the fqdn for TLS purpose	In the SCP implementation with NRF using TLS, notifications were not being received. This issue occurred because subscriptions were created using the IP address instead of the Fully Qualified Domain Name (FQDN), which was required by the NRF verification process. **Doc Impact**: There is no doc impact.	3	24.2.2
37634513	DiscardWithErrorRspCount parameter needs to be corrected in worker logs.	The `DiscardWithErrorRspCount` parameter in worker logs was incorrectly recorded. **Doc Impact**: There is no doc impact.	3	25.1.100
37632229	SBI Message Priority Rest API does not allow nftype as query parameter & PUT operation on existing rule is not allowed for change in scope of method array list	The SBI Message Priority REST API did not support `nftype` as a query parameter. Additionally, the PUT operation on an existing rule was not permitted when attempted to modify the scope of the method array list. **Doc Impact**: There is no doc impact.	3	25.1.100
37565543	SCP Alert triggered SCPEgressTrafficRoutedWithoutRateLimitTreatment without ERL enabled	In SCP 24.2.1, an alert for SCPEgressTrafficRoutedWithoutRateLimitTreatment was triggered, even though Egress Rate Limiting was not enabled. **Doc Impact**: There is no doc impact.	3	24.2.1

Table 4-14 (Cont.) SCP 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37439576	API Missing Validation for Mandatory Parameter: "enabled"	When a PUT request was made to the scp-features REST API, SCP did not return an error if the mandatory "enabled" parameter was missing. **Doc Impact**: There is no doc impact.	3	25.1.100
37428245	scp does not show profile details for NF-TYPE= SCP under edit profile option	When editing a profile for NF-TYPE=SCP, SCP did not display the profile details. **Doc Impact**: There is no doc impact.	3	25.1.100
37428201	scp returns misleading error when editing static nrf profiles	When editing static NRF profiles, SCP returned a misleading error message. **Doc Impact**: There is no doc impact.	3	25.1.100
37426620	SCP scp-subscription pod is generating WARN messages with "{Response is Successful but NO BODY found}"	In SCP 24.2.1, the SCP-Subscription pod generated WARN messages {Response is Successful but NO BODY found}". **Doc Impact**: There is no doc impact.	3	24.2.1
37407917	"Max Retry Attempts field" is saved as zero value in Routing options of Mediation tab.	When saving routing options in the Mediation tab, the "Max Retry Attempts" field was stored as a zero value, even if a different value was entered. **Doc Impact**: There is no doc impact.	3	25.1.100
36173358	SCP Unable to forward notification requests when request is received with FQDN at profile level and DNS is not configured to resolve the FQDN.	When a notification request was received with a Fully Qualified Domain Name (FQDN) at the profile level and the DNS was not configured to resolve the FQDN, SCP was unable to forward the request. **Doc Impact**: There is no doc impact.	3	23.3.0
38157537	SCP notification pod in CrashLoopBackOff state after OCCNE upgrade from 24.2.3 to 24.2.6	After upgrading CNE from 24.2.3 to 24.2.6, SCP-Notification pod entered a CrashLoopBackOff state, despite functioning correctly before the upgrade. **Doc Impact**: There is no doc impact.	3	24.2.3

Table 4-14 (Cont.) SCP 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38157409	SCP Worker pod continuous restarts due to Traffic Feed stackTrace java.lang.StringIndexOutOfBoundsException: begin 7, end 4	The SCP-Worker pod continuously restarted due to a Traffic Feed stack trace error, specifically a `java.lang.StringIndexOutOfBoundsException` with begin index 7 and end index 4. **Doc Impact**: There is no doc impact.	3	24.2.3
38143198	SCP not allowing to edit NRF record in NRF SRV configuration	SCP did not allow to edit NRF record in the NRF SRV configuration. **Doc Impact**: There is no doc impact.	3	25.1.100
38116473	Enhancement in metric ocscp_metric_scp_generated_response_total to get pegged for timeout and connection error from mediation ms.	The `ocscp_metric_scp_generated_response_total` metric did not accurately reflect timeout and connection errors from the mediation service, leading to incomplete data representation. **Doc Impact**: There is no doc impact.	3	24.2.0
38111599	Envoy filter configuration section needs to be corrected in 25.1.200 user guide of SCP	In the 25.1.200 *Oracle Communications Cloud Native Core, Service Communication Proxy Installation, Upgrade, and Fault Recovery Guide*, `name` and `type` fields were incorrectly documented for ASM configuration to allow the XFCC header. **Doc impact**: Updated the `name` and `type` fields for ASM configuration to allow the XFCC header in the "Deployment Configurations" section in *Oracle Communications Cloud Native Core, Service Communication Proxy Installation, Upgrade, and Fault Recovery Guide*.	3	25.1.100
38109905	ATS scenario is failing because duplicate registration observed on setnrfl1.nrfset.5gc.mnc012.mcc345 nrf post migration	Duplicate registrations were observed on the NRF setnrfl1.nrfset.5gc.mnc012.mcc345 after migration, causing the ATS scenario to fail. **Doc Impact**: There is no doc impact.	3	25.1.100

Table 4-14 (Cont.) SCP 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38073526	OCI threshold API returns error despite putting correct data.	The OCI threshold API returned an error when provided with accurate data, preventing successful threshold configuration. **Doc Impact**: There is no doc impact.	3	25.1.100
38034923	SCP User guide discrepancies	The metrics with dimension `ocscp_nf_service_name` were not updated to use `ocscp_nf_service_type` in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*. **Doc impact**: Replaced the dimension `ocscp_nf_service_name` with `ocscp_nf_service_type` in the "Metrics" section in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.	3	24.3.0
38030151	NrfBootStrapInfo: Heartbeat request is happening with old replaced nrf	SCP sent heartbeat requests using an outdated NRF instance that was replaced. **Doc Impact**: There is no doc impact.	3	25.1.100
38025580	NrfBootStrapInfo: Audit is happening with the old replaced nrf	During the audit process, SCP referenced outdated NRF information was previously replaced. **Doc Impact**: There is no doc impact.	3	25.1.100
37987680	On Dual stack setup, service entry for foreign SCP profile is getting created with ipv4 only.	In a dual stack setup, the service entry for a foreign SCP profile was incorrectly created using only IPv4, despite SCP's capability to support both IPv4 and IPv6. **Doc Impact**: There is no doc impact.	3	25.1.100
37954103	SCP not able to register mate SCP profile if capacity is not present in profile	SCP failed to register a secondary profile when the associated primary profile lacked the required capacity. **Doc Impact**: There is no doc impact.	3	25.1.100

Table 4-14 (Cont.) SCP 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37511517	During SCP overload scenario(200%), Request and Response processing time for SCP exceeded 2 seconds	While performing upgrade and rollback operations between SCP 23.4.x and 24.2.x, the request and response processing time exceeded the expected limit of 10 seconds. **Doc Impact**: There is no doc impact.	3	24.2.3
37779596	Error Message summary needs to be corrected in CNCC for NF Service Config Set	The Error Message summary required correction on the CNC Console for NF Service Config Set. **Doc impact**: There is no doc impact.	4	25.1.100
37779565	ocscp_notification_nf_profile_rejected_total metrics pegged with internal error in case of received invalid notification with mandatory parameter missing in request	The `ocscp_notification_nf_profile_rejected_total` metric remained pegged with an internal error when an invalid notification was received with a mandatory parameter missing in the request. **Doc Impact**: There is no doc impact.	4	25.1.100
37697207	Api root header with ipv6 without square bracket and no port gives 500.	When an API root header contained an IPv6 address without square brackets and no specified port, it returned response 500. **Doc Impact**: There is no doc impact.	4	25.1.100
37690826	Exceptions list is not updating properly under nextHopSEPP when one exception is passing the list	When one exception was passing through the list, the exceptions list under nextHopSEPP was not updated. **Doc Impact**: There is no doc impact.	4	25.1.100
37659775	clarification for Side Car Proxy Server Header	The following sidecar proxy server header behavior was observed: "SCP responds to client with “503” and "envoy" as server header". **Doc impact**: Added the "Understanding sideCarProxyServerHeader and sideCarProxyStatusCode Configurations" subsection in *Oracle Communications Cloud Native Core, Service Communication Proxy REST Specification Guide*.	4	23.4.3

Table 4-14 (Cont.) SCP 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37648525	Then Vender Specific Error ID for error resulted because of ConnectionFailed due to jetty client and ConnectionTimeout at SCP are same	A Vendor Specific Error ID was triggered due to a connection failure between Jetty client and SCP. The failure was caused by a connection timeout, and the error IDs for both the Jetty client and SCP were identical. **Doc impact**: Updated the Error ID OSCP-WRK-ROUTE-E002 in "Table 3-6 SCP-Worker Microservice Error IDs" in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.	4	25.1.100
37615522	Two subscription requests are sent for UDM, with TSI as NRF for UDM and LOCAL for the other NFs, in the upgrade setup from 24.3.0 to 25.1.100	During an upgrade from SCP 24.3.0 to 25.1.100, two subscription requests were sent to the UDM. One request used TSI as the NRF for the UDM, while the other used LOCAL for the remaining NFs. **Doc Impact**: There is no doc impact.	4	25.1.100
37585269	Error Message needs to be corrected on the Console GUI while configuring Consumer Info configuration	An incorrect error message appeared on the CNC Console when configuring Consumer Info configuration. **Doc Impact**: There is no doc impact.	4	25.1.100
37505826	SCP CNCC, NF Discovery Response Cache Configuration Rule screen should a have visible column for added Exclude Discovery Query Parameters	On the CNC Console, the NF Discovery Response Cache Configuration Rule section did not have a column to view added Exclude Discovery Query parameters. **Doc Impact**: There is no doc impact.	4	25.1.100
37407899	SCP returns incorrect error while modifying NRF Profile on SCP	When modifying an NRF profile on SCP, an incorrect error message was returned. **Doc Impact**: There is no doc impact.	4	25.1.100
37309676	dnnList missing from pcfInfo in PCF profile on CNCC GUI	In SCP 24.2.1, the `dnnList` field was missing from the `pcfInfo` section in the PCF profile when viewed on the CNC Console. **Doc Impact**: There is no doc impact.	4	25.1.100

Table 4-14 (Cont.) SCP 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37273615	SCP returns 500 internal error in case of action parameter missing from approuting options REST API request	When the action parameter was missing from the approuting options REST API request, SCP returned a 500 internal error. **Doc Impact**: There is no doc impact.	4	25.1.100
37043138	Getting ocscp_nf_setid as UNKNOWN instead of nf_setid of PCF in the metric ocscp_metric_http_rx_res_total	The `ocscp_metric_http_rx_res_total` metric displayed `ocscp_nf_setid` as UNKNOWN instead of the expected `nf_setid` of PCF. **Doc Impact**: There is no doc impact.	4	24.3.0
36714066	SCP OCI Recovery Validity Period Description in Console UI needs to be updated.	The description for SCP OCI Recovery Validity Period on the CNC Console required an update. **Doc Impact**: There is no doc impact.	4	24.2.0
38043000	Service Group Configuration for CHF	In SCP 24.3.0, the service group configuration for CHF was found to be incorrect. **Doc impact**: Removed the "Configuring Service Groups Parameters" section from *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.	4	24.3.0
37304141	nsiList values showing as NULL on CNCC GUI despite being set in SCP	The `nsiList` values appeared as NULL on the CNC Console, even though they were correctly set in SCP. **Doc Impact**: There is no doc impact.	4	25.1.100
37976004	SCP ATS Overall Results Report Misspells Feature as Featue	In SCP-ATS 25.1.100, the Overall Results Report incorrectly spelled "Feature" as "Featue." **Doc Impact**: There is no doc impact.	4	25.1.100

Table 4-14 (Cont.) SCP 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37966147	http and https port default needs to be updated in SCP installation guide	*Oracle Communications Cloud Native Core, Service Communication Proxy Installation, Upgrade, and Fault Recovery Guide* contained incorrect default port information for HTTP and HTTPS. **Doc impact**: Updated the port numbers of `scpProfileInfo.scpInfo.scpPorts.https` and `scpProfileInfo.scpInfo.scpPorts.http` Helm parameters in the "Global Parameters" section of *Oracle Communications Cloud Native Core, Service Communication Proxy Installation, Upgrade, and Fault Recovery Guide*.	4	25.1.100
37869819	Put request for NFServiceConfig doesn't trigger reconfiguration for old NFType/NFService	A PUT request for NFServiceConfig failed to trigger reconfiguration when the request involved an older NFType or NFService. **Doc Impact**: There is no doc impact.	4	25.1.100
37930930	SCP User Guide - Table A-1 HTTP Status Code Supported on SBI	The HTTP status codes supported on the SBI interface were not correctly updated in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*. **Doc impact**: Updated the "Table A-2 Additional Status Codes Applicable for Reroute Condition List (reRouteConditionList) " with correct HTTP status codes in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.	4	25.1.100

Note

Resolved bugs from 24.2.4 and 24.3.0 have been forward ported to Release 25.1.200.

Table 4-15 SCP ATS 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38128249	SCP0015 WS1.5 failed SCP_Subscription_SubscriptionWithNRFforNfTypeUDM_P0 - 062725	The test case failed while validating the nrf_subscription_delete request. **Doc Impact**: There is no doc impact.	3	25.1.100
38128999	SCP0015 WS1.5 failed SCP_EgressRateLimitingRelease16_AUSF_P0 - 062725	The scenario scenario-1_RateLimitingEgressAlternateRouteReverseLookup failed due to the metric metricfAUSF3 returning a value of 601 instead of 600. All the configurations were correct, but the test case failed due to the metric count exceeding the expected value. **Doc Impact**: There is no doc impact.	3	25.1.100

4.2.10 SEPP Resolved Bugs

Release SEPP 25.1.201

Table 4-16 SEPP 25.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38187650	CAT1 Feature Alerts are not coming in Prometheus GUI after sending invalid calls.	Alerts for the Cat-1 NRF Service API Query Parameters Validation feature were not triggering, despite error thresholds being exceeded during testing. This was due to the alert interval being incorrectly set to one minute in the alert configuration file. **Doc Impact:** Updated the alert expressions of Cat-1 NRF Service API Query Parameters Validation alerts in the *Oracle Communications Cloud Native Core, Security Edge Protection Proxy User Guide.*	3	25.1.100

Table 4-16 (Cont.) SEPP 25.1.201 Resolved Bugs

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

Table 4-16 (Cont.) SEPP 25.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38211747	SEPP 25.1.200 GA Package has incorrect cnDBTier CV file - RC4 File used instead	In the 25.1.200 SEPP GA Artifacts/ Scripts directory, the cnDBTier custom values file in use was `ocsepp_dbtier_25.1.200_custom_values_25.1.200.yaml`, which was incorrectly based on a pre-GA version. As per the deployment standards and release guidelines, the correct GA version of the cnDBTier custom values file should have been used. **Doc Impact**: There is no doc impact.	4	25.1.200
38198678	namespace hardcoded to sepp-namespace for pod status check alerts	In the SEPP User Guide,a note should have instructed users to update the sepp-namespace in alert file to the actual namespace where SEPP was deployed was missing. The absence of this information prevented all newly added alerts from being raised correctly. **Doc Impact:** Added a note to the Alert Configuration section of the *Oracle Communications Cloud Native Core, Security Edge Protection Proxy User Guide*.	4	25.1.200

Release SEPP ATS 25.1.201

Table 4-17 SEPP ATS 25.1.201 Resolved Bugs

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

Release 25.1.200

Table 4-18 SEPP 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37738503	SEPP returns 500 error, instead of configured one, when timestamp format does not meet the requirement	When the Cat-3 Previous Location Check feature was enabled, the authentication-status response from the UDR included a timestamp in the format `"timeStamp": "2018-01-02T08:17:14Z"`, which did not include milliseconds. As a result, the SEPP returned a 500 Internal Server Error instead of the expected 406 status code. **Doc Impact:** There is no doc impact.	3	25.1.100

Table 4-18 (Cont.) SEPP 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37744123	Intermittent NPE reported in pn32f logs at 10 TPS when Cat3 time check is enabled	A Null Pointer Exception was intermittently reported in pn32f logs when the Cat-3 Time Check for Roaming Subscribers feature was enabled and traffic was at 10 transactions per second (TPS). **Doc Impact:** There is no doc impact.	3	25.1.100
37669351	Need assistance to test Health Check Feature	When the peer monitoring configuration was modified, the SCP Health Check request rate increased. This behavior could be tracked using an alert expression `rate(oc_egressgateway_peer_health_ping_request_total {namespace=~"namespace"}[2m])`. **Doc Impact:** There is no doc impact. **Related Bug:** Gateway bug: 37727221	3	24.3.1
37755073	Too many TCP connections from SEPP to UDM	The PLMN Egress Gateway established a very high number of TCP connections towards the outbound Network Function UDM. This issue occurred because the PLMN Egress Gateway was opening a new TCP connection with almost every new request when the Jetty idle timeout was set to 0. **Doc Impact:** Added the note to the `jettyIdleTimeout` parameter in the "Timer Parameters" section in *Oracle Communications Cloud Native Core, Security Edge Protection Proxy Installation, Upgrade, and Fault Recovery Guide*. **Related Bug:** Gateway bug: 37765399	3	24.3.1

Table 4-18 (Cont.) SEPP 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37680589	SEPP TUH header path for deregistration notification does not work	SEPP failed to perform TUH (Topology Recovery) for `NFInstanceId` in the deregistration notification header path from the UDM to the AMF. SEPP did not perform TUH on the header path for the deregistration-notification callback. **Doc Impact:** Updated the path configurations in the "Topology Hiding" section in *Oracle Communications Cloud Native Core, Security Edge Protection Proxy User Guide*.	3	24.2.1
37514476	Message schema validation failing in SEPP	With the Cat-0 SBI Message Schema Validation feature enabled, the SEPP blocked requests sent from the visiting AMF to the Home UDM through the SEPP for the `/nudm-sdm/v2/{supi}` endpoint, returning a 406 error. The issue was raised because the SEPP's message validation schema was expected `dataset-names` to be enclosed in square brackets (`[]`). A similar issue was observed for the `/nnrf-disc` endpoint. However, according to 3GPP TS 29.501, `dataset-names` it is defined as an array of simple types, and the specification does not require square brackets or double quotes for formatting. **Doc Impact:** There is no doc impact.	3	24.2.0

Table 4-18 (Cont.) SEPP 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37499126	Ratelimit failing when header contains srcinfo	The header validation failed when the source information was included in the header. However, the validation succeeded when only the origin PLMN was present in the header. Failing Header: 3gpp-sbi-originating-network-id: 310-014; src: SEPPsepp001.sepp.5gc.mnc014.mcc310.3gppnetwork.org Working Header: 3gpp-sbi-originating-network-id: 310-014 **Doc Impact:** There is no doc impact.	3	23.1.1
37623689	SEPP 24.3.0 ATS CV file should not expose password	The ATS custom values file previously exposed passwords in the `custom-values.yaml` file. This issue was resolved by updating the ATS charts to ensure passwords are no longer exposed. **Doc Impact:** There is no doc impact.	3	24.3.0

Table 4-18 (Cont.) SEPP 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release

37916233	Update the SEPP ATS Guide. to add the withEnv configurations in the pipeline script	An error occurred when using customized ATS pipelines for SEPP NewFeatures and Regression. To resolve this issue, specific environment variables must be configured.
		Doc Impact:
		Added the following environment variables in *Oracle Communications Cloud Native Core, Automated Test Suite User Guide*:
		`withEnv([`
		`'TestSuite=Regression',`
		`'Execute_Suite=SEPP',`
		`'FilterWithTags=true,false',`
		`'Fetch_Log_Upon_Failure=NO',`
		`'Select_Features_Option=All',`
		`'Configuration_Type=Custom_Config'`
		`])`
			3	25.1.100

Table 4-18 (Cont.) SEPP 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37870171	CNDB metrics and alerts are not being fetched in Prometheus for the Hardhead1 cluster, and the corresponding namespace is not visible in the Grafana dashboard	Prometheus was not collecting CNDB-related metrics, which prevented CNDB alerts from firing. **Doc Impact:** Updated the `traffic.sidecar.istio.io/excludeInboundPorts: "8081,8080` exclusion in CNDB pods, as specified in *Oracle Communications Cloud Native Core, cnDBTier User Guide* in *Oracle Communications Cloud Native Core, Security Edge Protection Proxy Installation, Upgrade, and Fault Recovery Guide.*	3	25.1.100
37587256	Request guidance on how to accommodate for 2 and 3 digit MNCs for CAT2 screening in SEPP	In the Cat-2 Network ID Validation feature, rules were defined to filter specific requests. When configuring these rules, the length of the Mobile Network Code (MNC) had to be specified as either 2 or 3. Since there was only one rule for both directions, if the MNC lengths differed between the two countries, the filtering rule failed to work for one direction. **Doc Impact:** Updated the "Cat -2 Network ID Validation Feature" section with information about fetching MNC length from PLMN table in *Oracle Communications Cloud Native Core, Security Edge Protection Proxy User Guide*.	3	24.3.0

Table 4-18 (Cont.) SEPP 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release

38059326	Overload is enabled by default in CV, causing exceptions in IGW pod logs	By default, the following flag was enabled in the `ocsepp_custom_values_<version>.yaml`:
		
		`overloadManager:`
		`  enabled: true`
		`  nfType: 'sepp'`
		
		`ingressGatewaySvcName`
		`: n32-ingress-gateway`
		
		`ingressGatewayPort:`
		`80`
		
		This caused multiple exceptions in the `n32-ingress-gateway` pods because the feature was enabled, but the necessary configurations were not present.
		Doc Impact:
		The default value for the `overloadManager.enabled` is changed to **false** in *Oracle Communications Cloud Native Core, Security Edge Protection Proxy Installation, Upgrade, and Fault Recovery Guide.*
			3	25.1.100

37855789	coherence service log level change is not exposed via REST and CNCC	The log level for the Coherence service could not be changed through REST or CNC Console because the configuration option was not exposed. This prevented users from adjusting the log level as needed. **Doc Impact:** There is no doc impact.	3	25.1.100

Table 4-18 (Cont.) SEPP 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37670498	ERROR LOG in SEPP config manager pod and Performance pod	Continuous Error logs were observed in the SEPP `config-manager` pod and `performance` pod. • Config Manager Pod Logs: The pod continuously generated ERROR logs related to `connector/J`, suggesting the use of `autoreconnect=true` due to client timeout issues. • Performance Pod Logs: The pod was incorrectly sending curl requests to the n32-igw service on port 80, which was not exposed by the service. **Doc Impact:** There is no doc impact.	4	24.2.1
37720757	different validation for mcc on CNCC and REST for MCC Exception list	Different validation rules for the Mobile Country Code (MCC) were applied in CNC Configuration and REST API for the MCC Exception list. While CNC Configuration performed the validation correctly, the REST API accepted MCC values starting with 0, when triggered directly, which was incorrect. **Doc Impact:** There is no doc impact.	4	25.1.100

Table 4-18 (Cont.) SEPP 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36605004	OCSEPP: During installation SEPP 24.1.0 unwanted warnings are observed.	During SEPP deployment, warnings were thrown, although the deployment was successful. These warnings originated from the mediation common service and were related to attempts to overwrite table values with non-table data for the following configurations: • `ocsepp.k8sResource.container.prefix` • `ocsepp.k8sResource.container.suffix` • `ocsepp.nf-mediation.global.k8sResource.container.prefix` • `ocsepp.nf-mediation.global.k8sResource.container.suffix` **Doc Impact:** There is no doc impact.	4	24.1.0
37475488	Get request for non-existing trigger list has different behavior for Cat3 and Cat0/ Cat1/Cat2	A GET request for a non-existing list had inconsistent behavior across different categories. For Category 3 (Cat-3), SEPP responded with a 404 Not Found status, while for Categories 0, 1, and 2 (Cat-0/Cat-1/Cat-2), it responded with a 200 OK status. **Doc Impact:** There is no doc impact.	4	25.1.100

Table 4-18 (Cont.) SEPP 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37531696	coherence service logs are being printed at the DEBUG level even though the log level is set to INFO.	Coherence service logs were being printed with the label `DEBUG` despite the log level being set to `INFO` in both `ocsepp_custom_values_<version>.yaml` file and deployment configurations. This resulted in unnecessary flooding of logs. **Doc Impact:** Updated the default value of `coherence-svc.log.root` and `coherence-svc.log.sepp` parameters to **ERROR** in the Coherence section in *Oracle Communications Cloud Native Core, Security Edge Protection Proxy Installation, Upgrade, and Fault Recovery Guide*.	4	25.1.100
37553652	GET request for topology hiding header config is responded with status code 201	A GET request for the topology hiding header configuration returned an HTTP status code of 201. According to the specification, the status code for a GET request should be 200 OK instead of 201. This discrepancy caused the HTTP response status code to deviate from the expected behavior. **Doc Impact:** Added the REST API details for header and body GET request for configuring Topology Hiding feature in *Oracle Communications Cloud Native Core, Security Edge Protection Proxy REST Specification Guide*.	4	25.1.100

Table 4-18 (Cont.) SEPP 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37647484	Next-hop header with wrong value	The next-hop header for n32f traffic did not contain the correct Fully Qualified Domain Name (FQDN). Upon analysis, it was determined that the `x-next-hop` header, a custom header, was not being used in n32f traffic routing. As a result, this header was removed when n32f traffic was exchanged to resolve the issue. **Doc Impact:** There is no doc impact.	4	24.3.1
37713281	"Blocklist Refresh Time Unit" default value is blank even though it is mandatory	The Blocklist Refresh Time Unit field had a blank default value, despite being a mandatory field. This caused the Cat-3 Time Check options page to fail to save when using default configurations. The issue stemmed from the absence of a default value for this field. Users were unable to save the Cat-3 Time Check for Roaming Subscribers options page with default values due to the missing default value for "Blocklist Refresh Time Unit." **Doc Impact:** Updated the Cat-3 Time Check for Roaming Subscribers feature section with information about blocklist functionality In *Oracle Communications Cloud Native Core, Security Edge Protection Proxy User Guide.*	4	25.1.100

Table 4-18 (Cont.) SEPP 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37713498	Default value of "Average Flight Velocity (km/hr)" should be realistic value	The default value for "Average Flight Velocity (km/hr)" was set to 1,20,000, which was unrealistic and could lead to misconfiguration. The default value was updated to a more realistic figure to prevent potential issues. **Doc Impact:** The default value of Average Flight Velocity is set as 12000 km/hr in the Cat-3 Time Location Check for Roaming Subscribers section of *Oracle Communications Cloud Native Core, Security Edge Protection Proxy User Guide* and *Oracle Communications Cloud Native Core, Security Edge Protection Proxy REST Specification Guide.*	4	25.1.100
37720181	detail and cause attribute shall be updated in response if mcc is invalid	In the Cat-3 Time check feature, when a wrong MCC (Mobile Country Code) was provided in the configuration, the response included misleading information in the cause and detail attributes. The response incorrectly stated that the MCC could be between 0 and 3, which was not accurate. **Doc Impact:** There is no doc impact.	4	25.1.100

Table 4-18 (Cont.) SEPP 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37834640	content-type http header is being sent in case TimeCheck is failed with 200 response code	During a failed Cat-3 Time Check scenario, the system incorrectly sent a `Content-Type` HTTP header with a 200 response code. The issue occurred when an authentication request with SUPI was sent to the UDR, but the request failed due to the UDR being down, resulting in an exception. The SEPP returned a 200 OK response as configured for the consumer. While the response body was empty, the presence of the `Content-Type` header misleadingly suggested that a body was included. **Doc Impact:** There is no doc impact.	4	25.1.100

Table 4-18 (Cont.) SEPP 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37854672	Critical alert criteria for Cat3 Time check feature shall be updated	Critical alert criteria for Cat-3 Time Check feature shall be updated. Critical alert criteria for Cat3 Time check feature shall be updated. Only minimum criteria shall be there, not the upper limit for critical alert. If the failures are more than 3000 in the given window, then the critical alert won't be raised. Hence the upper limit shall be removed. Alert names: pn32fTimeUnauthLocChkValFailAlrtCritical and pn32fTimeUnauthLocChkExcepFailAlrtCritical Criteria for critical alerts: • ocsepp_time_unauthenticated_location_exception_failure_total offset 2m) <= 3000 • ocsepp_time_unauthenticated_location_validation_failure_total offset 2m) <= 3000 The critical alert criteria for the Cat-3 Time Check feature were updated. The criteria now include only a minimum threshold, removing the upper limit for critical alerts. If the number of failures exceeds 3000 within the specified window, a critical alert will not be raised. This change applies to the alerts named `pn32fTimeUnauthLocChkValFailAlrtCritical` and `pn32fTimeUnauthLocChkExcepFailAlrtCritical`. The updated criteria for critical alerts are as follows: • `ocsepp_time_unauthenticated_location_exception_failure_total (offset 2m) <=3000` • `ocsepp_time_unauthenticated_location_validation_failure_t`	4	25.1.100

Table 4-18 (Cont.) SEPP 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
		`otal (offset 2m) <=3000` **Doc Impact:** Updated the expressions of the following alerts in the "Cat-3 Time Check for Roaming Subscribers Alerts "section of *Oracle Communications Cloud Native Core, Security Edge Protection Proxy User Guide*: • `pn32fTimeUnauthLocChkValFailAlrtCritical` • `pn32fTimeUnauthLocChkExcepFailAlrtCritical`		
37880515	peer_domain dimention is not getting dumped in "ocsepp_time_unauthenticated_location_blacklist_requests_total"	In previous releases, the metric `ocsepp_time_unauthenticated_location_blacklist_requests_total` did not include the `peer_domain` dimension, despite the User Guide specifying that it should be present. This issue was resolved by adding the `peer_domain` value to the metric, ensuring compliance with the documentation. **Doc Impact:** There is no doc impact.	4	25.1.100

Table 4-18 (Cont.) SEPP 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38011729	SEPP GET configuration returns 201 Created for TH query	During testing of SEPP release 25.1.100, it was observed that a GET command to a specific REST API resource incorrectly returned a 201 Created response code. This behavior is unexpected, as a GET request should typically return a 200 OK response code when the resource is successfully retrieved. **Doc Impact:** Updated the REST API details in the "Topology Hiding" section in *Oracle Communications Cloud Native Core, Security Edge Protection Proxy REST Specification Guide*.	4	25.1.100

Table 4-18 (Cont.) SEPP 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37902132	Missing "s" on response for ocsepp_pn32f_response_total	In the `sepp_Customconfigtemplates_24.3.1.zip` file, the metric name `ocsepp_pn32f_response_total` was incorrectly spelled without the final "s" in the files `ocsepp_dashboard.json` and `ocsepp_dashboard_promha.json`. The correct metric name should be `ocsepp_pn32f_responses_total`. This issue was present in the following lines: • ocsepp_dashboard.json: – Line 1291: `"expr": "(sum(ocsepp_pn32f_response_total)/ sum(ocsepp_pn32f_requests_total))*100"` – Line 1539: `"expr": "sum(irate(ocsepp_pn32f_response_total[2m]))"` • ocsepp_dashboard_promha.json: – Line 5563: `"expr": "sum((ocsepp_pn32f_response_total{namespace=~\"$Namespace\"}))by(app,status_code)"` **Doc Impact:** There is no doc impact.	4	24.3.1
37987985	Apply CNCESSEPP-849 fix to all cat3 time check metrics	The `peer_domain` dimension was added to all Cat-3 Time Check for Roaming Subscribers metrics, and the correct value was populated for this dimension. This update ensures that the metrics accurately reflect the `peer_domain` information. **Doc Impact:** There is no doc impact.	4	25.1.100

Table 4-18 (Cont.) SEPP 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37719644	response for an invalid value of "avgFlightVelocity" in the configuration is incorrect	When an invalid value for the `avgFlightVelocity` parameter was provided in the configuration, the system incorrectly returned a 400 response code instead of the configured response code. Additionally, the `Content-Type` header in the response was set to `application/json`, whereas it should have been `application/problem+json` to comply with the expected format for error responses. **Doc Impact:** There is no doc impact.	4	25.1.100
37713670	response for an invalid value of "messageFilteringOnUnAuthLocationEnabled" in the configuration is incorrect	When an invalid value for the `messageFilteringOnUnAuthLocationEnabled` parameter was provided in the configuration, the system incorrectly returned a 400 response code instead of the configured response code. Additionally, the `Content-Type` header in the response was set to `application/json`, whereas it should have been `application/problem+json` to comply with the expected format for error responses. **Doc Impact:** There is no doc impact.	4	25.1.100

Table 4-18 (Cont.) SEPP 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38047999	Description shall be updated for SoR Config Allowed List config	The REST API documentation contained inaccuracies in the table describing the SoR Config Allowed List. Specifically: 1. The description for the PUT method row was incorrectly stated as *"Configures Mediation trigger point configuration for given data."* This description does not align with the purpose of the SoR Config Allowed List. 2. In section 2.21, the term "Allowed List" was used instead of the correct term "Trigger Rule List." The document was updated to correct these issues, ensuring accurate and consistent terminology. **Doc Impact:** Updated the following in *Oracle Communications Cloud Native Core, Security Edge Protection Proxy REST Specification Guide:* • Updated the name of the REST API as SOR Config Trigger Rule List. • Updated the description of PUT method in SOR Config Trigger Rule List.	4	25.1.100

Table 4-18 (Cont.) SEPP 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38048136	Deleting a non-existing SoR trigger list returns 400 instead of 404	When the DELETE RES API was used to delete a non-existing SoR trigger list, a mismatch was observed between the HTTP response status code and the error message in the response body. The HTTP response status code returned was 400 (Bad Request), while the error message in the response body indicated a 404 (Not Found) status. The error message specifically stated, "404 NOT_FOUND 'sor trigger list Name is missing in DB'." **Doc Impact:** There is no doc impact.	4	25.1.100

Note

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

4.2.11 UDR Resolved Bugs

Release 25.1.200

Table 4-19 UDR 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37814291	UDR:How to specify resources for each container in Bulk-Import	During Subscriber Bulk Import Tool deployment, the users were unable to specify resources for individual containers in the configuration. Each container was deployed with the same CPU and memory resources (6 CPU and 7Gi memory), leading to excessive resource utilization when all containers were deployed. **Doc Impact:** Updated the total CPU and total Memory for the nudrbulkimport Microservice in the "Resource Requirements for UDR Tools" section in *Oracle Communications Cloud Native Core, Unified Data Repository Installation, Upgrade, and Fault Recovery Guide*.	3	24.2.0
37777519	SLF - Not able to change the loglevel for nrfClientManagement service	In the 25.1.100 release of SLF, users were unable to change the log level for the nrfClientManagement service from the CNC Console. When attempting to change the log level from WARN to DEBUG, an error occurred in the NrfClientManagement pod and the log level was not updated in the NrfClient pod. **Doc Impact:** There is no doc impact.	3	25.1.100

Table 4-19 (Cont.) UDR 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37590048	OCUDR:snmp MIB Complain from SNMP server	In the SLF, EIR, and UDR Management Information Base (MIB), users encountered an issue when loading them into an Simple Network Management Protocol (SNMP) server. The SSNMP notifier was appending a ".1" suffix to the SNMP trap, resulting in an error. **Doc Impact:** There is no doc impact.	3	24.2.0
37501534	SLF_Controlled_shutdown not working after helm upgrade	In the 24.2.0 release of SLF, the Controlled Shutdown feature was not working as expected after a Helm upgrade. When attempting to apply a controlled shutdown from the CNC Console, SLF remained in the registered state and did not transition to the suspended state. Error messages were observed in the app Info logs, indicating an inability to get the operational state, and in the nudr-config logs, indicating an invalid URI sent from the client. **Doc Impact:** There is no doc impact.	3	24.2.0
37462379	NSSF - Customer facing ASM install issue	The user encountered a YAML parse error when attempting to install Aspen Service Mesh (ASM) using the provided charts. The error occurred due to a missing key in the envoy filter configuration of the service mesh resource yaml file. **Doc Impact:** There is no doc impact.	3	24.2.0

Table 4-19 (Cont.) UDR 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37785011	DIAMGW POD restart observed while running peformance for 10K SH & 17.2K N36 for 24 Hours with DB restart	In a performance test running for 24 hours with 10K SH and 17.2K N36, the diameter gateway pod was observed to restart multiple times. The restarts were caused by an Out of Memory (OOM) error, which resulted in the pod being terminated and restarted. **Doc Impact:** There is no doc impact.	3	25.1.100
37884685	Incorrect Metrics Mapping for diam_conn_local and diam_conn_network in UDR Namespace	The diam_conn_local and diam_conn_network were incorrectly mapped, leading to misinterpretation of system health and peer connectivity. **Doc Impact:** There is no doc impact.	3	24.2.0
37955075	Missing excludeInboundPorts and excludeOutboundPorts in EGW and Alternate-Route	The excludeInboundPorts and excludeOutboundPorts annotations were missing in the Egress Gateway (EGW) and Alternate-Route sections in the custom value yaml file. **Doc Impact:** There is no doc impact.	3	25.1.100
37883833	SLF 25.1.100 Servicemesh - Envoy filter need to be updated	In release 25.1.100, Jetty HTTP/2 client connections would hang due to high stream IDs. This occurred in long-lived connections with a high volume of requests, causing outbound traffic to stop until the server-side Istio sidecar terminated the connection due to idle timeout. The issue was resolved by updating the Envoy filter. **Doc Impact:** There is no doc impact.	3	25.1.100

Table 4-19 (Cont.) UDR 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37915245	SLF 25.1.100 REST API Configuration for nfscoring is missing in guide	The REST API configuration details for *nfscoring* were missing from the UDR documentation. **Doc Impact:** Updated REST API configuration of `nfscoring` in the "Configuration APIs for Common Services" section in *Oracle Communications Cloud Native Core, Unified Data Repository REST Specification Guide*.	3	25.1.100
38022882	Ingress Gateway Provisioning Pods Restarting in UDR 24.2.4 Under Load	In UDR version 24.2.4, ingress gateway provisioning pods were observed to restart continuously under load during test validation. This issue occurred at approximately 50 transactions per second (TPS) and was accompanied by log entries indicating "Error occurred in Netty Inbound Handler for address." **Doc Impact:** There is no doc impact.	3	24.2.4
37532285	Subscriber trace is missing for "400 Bad request " response of Duplicate POST Request	The subscriber trace was missing for a "*400 Bad Request*" response that occurred when a duplicate POST request was made. The issue occurred when the Allow Subscription Recreation feature was set to false. **Doc Impact:** There is no doc impact.	4	25.1.100

4.2.12 Common Services Resolved Bugs

4.2.12.1 ATS Resolved Bugs

Release 25.1.200

Table 4-20 ATS 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37882146	Require refinement in istio-proxy container applogs	When application logs were collected for the istio-proxy container, all the logs appeared in a single line, making them unreadable. **Doc Impact:** There is no doc impact.	4	25.1.100

4.2.12.2 ASM Configuration Resolved Bugs

Release 25.1.200

Table 4-21 ASM Configuration 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37883833	SLF 25.1.100 Servicemesh - Envoy filter need to be updated	In release 25.1.100, Jetty HTTP/2 client connections would hang due to high stream IDs. This occurred in long-lived connections with a high volume of requests, causing outbound traffic to stop until the server-side Istio sidecar terminated the connection due to idle timeout. The issue was resolved by updating the Envoy filter.	3	25.1.100
38000246	SLF 25.1.100 Servicemesh resource template is missing some of the required parameters	In releases 25.1.100, the servicemesh resource template was missing parameters required for configuring Envoy filters.	3	25.1.100

4.2.12.3 Alternate Route Service Resolved Bugs

Release 25.1.201

There are no resolved bugs in this release.

Release 25.1.200

There are no resolved bugs in this release.

4.2.12.4 Egress Gateway Resolved Bugs

Release 25.1.201

Table 4-22 Egress Gateway 25.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37574756	Metric occnp_oc_egressgateway_http_requests_total Shows NFServiceType & NFType as "UNKNOWN" for update_notify Request	The `occnp_oc_egressgateway_http_requests_total` metric displayed the `NFServiceType` and `NFType` fields as "UNKNOWN" for `update_notify` requests. **Doc Impact:** There is no doc impact.	3	25.1.200

Release 25.1.200

Table 4-23 Egress Gateway 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37685576	Flooded with IRC Exception warn messages in EGW	After editing the traffic.sidecar.istio.io/excludeInboundPorts or traffic.sidecar.istio.io/excludeOutboundPorts values in Egress Gateway deployment and service, occasional IllegalReferenceCountException warning messages were observed, though the issue was not consistently reproducible across multiple runs. **Doc Impact:** There is no doc impact.	2	24.2.11
37828830	Stream ID exhaustion in Jetty will result in stale and unused connection	Jetty experienced stream ID exhaustion, leading to the retention of stale and unused connections. **Doc Impact:** There is no doc impact.	2	25.1.200
37732048	EGW re-route is not happening to alternate SCP, it is re-routing to the same SCP where the error response was received	Egress Gateway failed to re-route requests to an alternate SCP after receiving an error response from the initial SCP. **Doc Impact:** There is no doc impact.	2	25.1.200

Table 4-23 (Cont.) Egress Gateway 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37766559	EGW not rerouting request, reporting 'Host already tried' and returning 503 as all peers are ineligible	Egress Gateway failed to reroute a request because it had already attempted the designated host, resulting in a "Host already tried" error. **Doc Impact:** There is no doc impact.	2	25.1.200
37403771	NRF upgrade failed with igw post upgrade hooks in error state	During the NRF upgrade, the process encountered an issue where the Ingress Gateway post-upgrade hooks entered an error state. **Doc Impact:** There is no doc impact.	2	23.4.10
37480520	After successful update of certificate in NRF k8S by OCCM by recreate process new certificate validity is not used in TLS handshake by NRF GWDuring the recreation process initiated by OCCM to update the certificate in the NRF Kubernetes environment, the new	During the recreation process initiated by OCCM to update the certificate in the NRF Kubernetes environment, the new certificate's validity was not utilized in the TLS handshake by NRF. **Doc Impact:** There is no doc impact.	2	25.1.100
37009578	Fix to provide an option to enable use of APIGW custom Jetty code instead of Jetty Library APIs for the Peer Monitoring feature	The Peer Monitoring feature relied on Jetty Library APIs instead of Gateway Services custom Jetty code. **Doc Impact:** There is no doc impact.	2	23.4.4

Table 4-23 (Cont.) Egress Gateway 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37559723	EGW not pegging metric occnp_oc_egressgateway_peer_health_status when DNS entries changed untill SCP health status change	The Egress Gateway failed to update the `occnp_oc_egressgateway_peer_health_status` metric when DNS entries were modified, resulting in stale health status information. **Doc Impact:** There is no doc impact.	3	25.1.200
37603838	Metric oc_egressgateway_peer_health_ping_request_total does not increment when switching between dynamic and static peer configuration	The metric `oc_egressgateway_peer_health_ping_request_total` failed to increment when switching between dynamic and static peer configurations. **Doc Impact:** There is no doc impact.	3	25.1.200
37611042	EGW Not Sending Error Response Body for 406 NOT_ACCEPTABLE During SBI Routing.	Egress Gateway did not send error response body for 406 NOT_ACCEPTABLE during SBI routing. **Doc Impact:** There is no doc impact.	3	25.1.100

Table 4-23 (Cont.) Egress Gateway 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37642234	After restarting EGW pods multiple times, Prometheus is not showing EGW outgoing connections.	After restarting Egress Gateway pods multiple times, Prometheus failed to display the outgoing connections from the Egress Gateway. **Doc Impact:** There is no doc impact.	3	24.2.4
37529542	Requests rejected by EGW local rate limiting not reflected in main EGW request metrics	Requests that were rejected due to local rate limiting by Egress Gateway were not accurately recorded in the main Egress Gateway request metrics. **Doc Impact:** There is no doc impact.	3	24.2.10
35923113	Incorrect peer Health Status when peerConfiguration consists of virtualHost and peerMonitoring is enabled	Egress Gateway displayed an incorrect peer health status when the peer configuration included a virtual host and peer monitoring was enabled. **Doc Impact:** There is no doc impact.	3	23.3.3
37733235	EGW Peer monitoring service is not working as expected	Egress Gateway peer monitoring service failed to function as intended. **Doc Impact:** There is no doc impact.	3	25.1.200

Table 4-23 (Cont.) Egress Gateway 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37780691	Metric oc_egressgateway_http_responses_total - Dimension errorReason changed from "All peers are Unhealthy." to "All peers are Ineligible."	In the `oc_egressgateway_http_responses_total` metric, the `errorReason` dimension incorrectly displayed "All peers are Unhealthy." **Doc Impact:** There is no doc impact.	3	25.1.200
37306243	Incorrect user-agent info sent by EGW , when access-token request sent towards NRF. (But when subsequent request sent towards Producer NF's , EGW properly sent the User-Agent info)	When sending an access-token request to NRF, Egress Gateway incorrectly sent the user-agent information. **Doc Impact:** There is no doc impact.	3	24.2.0
37527834	BlackListing of a Peer (configured as IP:port) in sbiRouting is not happening when reroute attempts is 0	When a peer was configured as an IP:port in sbiRouting, blacklisting did not occur even though the reroute attempts were set to 0. **Doc Impact:** There is no doc impact.	3	25.1.200

Table 4-23 (Cont.) Egress Gateway 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release

37527954	when 3gpp-sbi-target-apiroot and oc-alternateroute-attempt headers are sent in the request the peer selection is inconsistent with oc-alternateroute-attempt header value.	When both
		
		`3gpp-sbi-target-apiroot`
		
		and
		
		`oc-alternateroute-attempt`
		
		headers were included in the request, the peer selection did not consistently align with the value specified in the
		
		`oc-alternateroute-attempt`
		
		header.
		Doc Impact:
		There is no doc impact.
			3	25.1.200

37528604	EGW selects low-priority SCP when higher-priority SCP is available after blacklisting SCP1	Egress Gateway selected a low-priority SCP instead of an available higher-priority SCP after blacklisting SCP1. **Doc Impact:** There is no doc impact.	3	25.1.200

Table 4-23 (Cont.) Egress Gateway 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37355062	occnp_oc_egressgateway_peer_health_status reports incorrect peer health from one pod	The *occnp_oc_egressgateway_peer_health_status* metric inaccurately reported the health status of a peer from one pod. **Doc Impact:** There is no doc impact.	3	23.4.3
37501092	Egress Gateway not retrying to sameNRF or Next NRF when "errorCodes: -1" for errorSetId: 5XX on retryErrorCodeSeriesForNex/SametNrf OauthClient configuration.	Egress Gateway failed to retry requests to the same NRF or the next NRF when encountering an error code of "-1" within the 5XX error set, as specified in the retryErrorCodeSeriesForNext/SameNrf OauthClient configuration. **Doc Impact:** There is no doc impact.	3	24.2.5
37451580	Metric not getting pegged after health ping request is sent towards a peer.	The metric failed to register after a health ping request was sent to a peer. **Doc Impact:** There is no doc impact.	4	24.2.9
35412487	[FORWARD PORTING] Scheduler resiliency feature	During Web-Scale upgrade, scaling down and then scaling up the AM-PCF caused the PCF-EGW to return 500 errors. **Doc Impact:** There is no doc impact.	4	22.4.3

Table 4-23 (Cont.) Egress Gateway 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37617517	FQDN scheme probing with Alternate Route Service failed due to strict "scheme" check in EGW	FQDN scheme probing with Alternate Route Service failed because Egress Gateway enforced a strict check on the "scheme" parameter. **Doc Impact:** There is no doc impact.	4	24.2.12
37756514	Pod-protection :- Congestion Configuration refreshInterval default value showing 5000 instead of 500 and Observed NPE if we configure 50000ms	In the pod protection congestion configuration, the default value for refreshInterval was incorrectly displayed as 5000 milliseconds instead of 500 milliseconds. **Doc Impact:** There is no doc impact.	4	25.1.200

Note

Resolved bugs from 24.2.5 and 25.1.100 have been forward ported to Release 25.1.200.

4.2.12.5 Ingress Gateway Resolved Bugs

Release 25.1.201

Table 4-24 Ingress Gateway 25.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37887251	GW POP25 not able to accept/ discard request wrt percentages allocated to each route	The Ingress Gateway Pod Protection using Rate Limiting feature failed to accept or discard requests based on the predefined percentage allocations assigned to each route. **Doc Impact:** There is no doc impact.	2	25.1.200
37733322	PCF is sending Error Code 404 Not Found without any error cause if an invalid URI is present in AM-Create	Policy returned an HTTP 404 Not Found error code without including an error cause when an invalid URI was detected in the AM-Create request. **Doc Impact:** There is no doc impact.	3	25.1.200

Table 4-24 (Cont.) Ingress Gateway 25.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37574756	Metric occnp_oc_egressgateway_http_requests_total Shows NFServiceType & NFType as "UNKNOWN" for update_notify Request	The `occnp_oc_egressgateway_http_requests_total` metric displayed the `NFServiceType` and `NFType` fields as "UNKNOWN" for `update_notify` requests. **Doc Impact:** There is no doc impact.	3	25.1.200
37893522	IGW pre upgrade hooks error when convertHelmRoutesToREST flag is set to true and POP25 configs are added in HELM values.yaml	During the pre-upgrade process, Ingress Gateway hooks encountered an error when the `convertHelmRoutesToREST` parameter was enabled. **Doc Impact:** There is no doc impact.	3	25.1.200
34609077	Security issue for reloading certificate	The exposed API (reload or certificate) at the public service port of Ingress Gateway was not secured. **Doc Impact:** There is no doc impact.	3	24.3.0

> **Note**
>
> Resolved bugs from 24.2.0 have been forward ported to Release 25.1.201.

Release 25.1.200

Table 4-25 Ingress Gateway 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37820163	Pod-protection :- Pod protection feature is not functioning when IGW response with 4XX (400 and 404) Result code	The pod protection feature failed to function when the Ingress Gateway responded with 4XX (400 and 404) result codes. **Doc Impact:** There is no doc impact.	2	25.1.200
37859082	Pod-protection :- one of the pod struct at congestion level3 state during 53K traffic with 3000 fillrate and 25 replicas	During high congestion levels (level 3) with a traffic rate of 53K, a pod structure experienced issues when configured with a fill rate of 3000 and 25 replicas. This configuration led to unexpected behavior in the pod's operation under those specific conditions. **Doc Impact:** There is no doc impact.	2	25.1.200
37859129	Pod-protection :- During 12hrs of run for 53K traffic with fill rate 3000 and 25 replicas multiple exceptions are observed	During a 12-hour test run with 53,000 traffic requests, a fill rate of 3,000, and 25 replicas, the pod-protection system encountered multiple exceptions. **Doc Impact:** There is no doc impact.	2	25.1.200

Table 4-25 (Cont.) Ingress Gateway 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37852033	REST call podProtectionByRateLimiting API failed to update the configuration	The REST call to the `podProtectionByRateLimiting` API failed to update the configuration due to an internal processing error. **Doc Impact:** There is no doc impact.	2	25.1.200
37697053	When overload control feature with Local discard is enabled there is approximately 1 percent extra traffic discard as set by the load level	When the overload control feature with Local discard was enabled, it increased traffic discard, resulting in approximately 1% more traffic being discarded than the configured load level. **Doc Impact:** There is no doc impact.	2	25.1.200
37359902	Success percentage drops to 47-52% during in-service upgrade/ rollback of IGW from 24.3.3 to 25.1.0 and vice-versa	During in-service upgrade or rollback between Ingress Gateway 24.3.3 and 25.1.0, the success percentage dropped to 47-52%. **Doc Impact:** There is no doc impact.	2	25.1.100
37669166	IGW is adding wrong format of sbi-timer headers which is causing parsing error in NRF-Discovery at 1 CPS impacting NRF performance	Ingress Gateway incorrectly formatted sbi-timer headers, which resulted in parsing errors within the NRF-Discovery module. **Doc Impact:** There is no doc impact.	2	25.1.200

Table 4-25 (Cont.) Ingress Gateway 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37828830	Stream ID exhaustion in Jetty will result in stale and unused connection	Jetty experienced stream ID exhaustion, leading to the retention of stale and unused connections. **Doc Impact:** There is no doc impact.	2	25.1.200
37601685	IGW - High CPU when reset streams are triggered	High CPU usage occurred when reset streams were triggered due to inefficient resource management during the reset process. **Doc Impact:** There is no doc impact.	2	24.2.12
37480520	After successful update of certificate in NRF k8S by OCCM by recreate process new certificate validity is not used in TLS handshake by NRF GW	During the recreation process initiated by OCCM to update the certificate in the NRF Kubernetes environment, the new certificate's validity was not utilized in the TLS handshake by NRF. **Doc Impact:** There is no doc impact.	2	25.1.100
37487536	OCI/LCI header support not working with default configuration	In the default configuration, the OCI or LCI header support failed to function as intended. **Doc Impact:** There is no doc impact.	2	25.1.100

Table 4-25 (Cont.) Ingress Gateway 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37780732	Pod-protection :- Denied traffic is rejected even though congestion level is not reached	When the Pod Protection feature was enabled, traffic was incorrectly denied even though the congestion level had not been reached. **Doc Impact:** There is no doc impact.	2	25.1.200
37506720	Overload Discard Percentage for NRF Microservices	When a single Ingress Gateway microservice acted as a front end for both the NRF Access Token and Discovery microservices, the global configuration for sampling interval and token fetching was not performant due to the significant difference in incoming traffic volume between the two microservices. **Doc Impact:** There is no doc impact.	2	24.2.11
37365106	Pod Protection using Rate Limiting :- ASM enabled :- 401 unauthorized metric not updated in "oc_ingressgateway_http_responses_total"	When the Pod Protection using Rate Limiting feature was enabled with ASM, the *oc_ingressgateway_http_responses_total* metric failed to update with the 401 unauthorized response count. **Doc Impact:** There is no doc impact.	3	25.1.100

Table 4-25 (Cont.) Ingress Gateway 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37603838	Metric oc_egressgateway_peer_health_ping_request_total does not increment when switching between dynamic and static peer configuration	The metric `oc_egressgateway_peer_health_ping_request_total` failed to increment when switching between dynamic and static peer configurations. **Doc Impact:** There is no doc impact.	3	25.1.200
36091942	errorCodeSeriesId that is already in use at global level / routes level configuration should not be allowed to be removed using PUT/PATCH	Ingress gateway incorrectly allowed the removal of an `errorCodeSeriesId` that was already present at the global or route level configuration through PUT or PATCH requests. **Doc Impact:** There is no doc impact.	3	23.4.2
37855426	Pod-protection :- Observed Internal server error During pod-up if traffic comes more than fill rate - "Internal Server Error errorMessage: Cannot invoke \"ocpm.cne.gateway.util.congestion.CongestionLevel.value"	An internal server error occurred during pod startup when incoming traffic exceeded the fill rate, causing the system to fail to invoke the congestion level value method. **Doc Impact:** There is no doc impact.	3	25.1.200

Table 4-25 (Cont.) Ingress Gateway 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37882318	Issues while switching from HELM based routesConfig to REST based using convertRestToHelm flag	When switching from HELM-based routesConfig to REST-based configuration using the convertRestToHelm parameter, Ingress Gateway encountered issues, leading to unexpected behavior. **Doc Impact:** There is no doc impact.	3	25.1.200
37526295	In IGW:25.1.100, after enabling the CCA header a WARN log should be printed for the case where issue at age (iat) is greater than present time.	After enabling the CCA header, the system failed to print a WARN log when the issue at age (iat) was greater than the present time. **Doc Impact:** There is no doc impact.	3	25.1.100
35983677	NRF- Missing mandatory "iat claim" parameter validation is not happening in CCA header for feature - CCA Header Validation	In the CCA Header Validation feature, the system failed to validate the mandatory "iat claim" parameter, which was absent in the header. **Doc Impact:** There is no doc impact.	3	23.2.0
37864290	IGW accepting traffic above fillRate for POP25	When the FillRate was set to 1000 and deniedRequestAction was left unspecified, Ingress Gateway received 1050 TPS on the /nnrf-nfm/v1/nf-instances/ path. **Doc Impact:** There is no doc impact.	3	25.1.200

Table 4-25 (Cont.) Ingress Gateway 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37451885	IGW Helm Charts do not pass Yaml Lint	During a YAML lint scan initiated, the CNC Console identified compliance issues in Ingress Gateway Helm charts. **Doc Impact:** There is no doc impact.	3	25.1.100
37515236	Pod Protection using Rate Limiting :- ASM enabled :- HTTP request metrics is not getting pegged but Http response are updated when IGW reject with " Scheduler unavailable "	When Pod Protection with Rate Limiting was enabled in ASM, HTTP request metrics were not updated, even though HTTP response metrics were correctly updated when the Ingress Gateway rejected requests with a "Scheduler unavailable" error. **Doc Impact:** There is no doc impact.	3	25.1.100
37808385	Pod-protection :- Deniedaction-priority taking out of range values in REST Mode but same its working in HELM Configuration	In the REST mode, the Pod Protection feature incorrectly refused actions due to out-of-range values in the action-priority configuration. This issue did not occur in the HELM configuration, where the same settings functioned as expected. **Doc Impact:** There is no doc impact.	3	25.1.200

Table 4-25 (Cont.) Ingress Gateway 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37780770	Pod-protection :- CongestionConfig.levels.resources.onset should be more than abatement	In the Pod Protection configuration, the `CongestionConfig.levels.resources.onset` value was set to be less than the `abatement` value. **Doc Impact:** There is no doc impact.	3	25.1.200
36833538	User-Agent feature flag is enabled from CV file even we set the configMode as REST instead of HELM	The userAgent parameter was incorrectly enabled from the custom values file when the configuration mode was set to REST, rather than HELM. **Doc Impact:** There is no doc impact.	3	24.2.4
37483564	Null Pointer Exception in pegging response_processing_latency in IGW	A null pointer exception occurred while processing response latency in Ingress Gateway. **Doc Impact:** There is no doc impact.	3	23.4.6
36672456	WARNING level displayed as BLANK on Discard Policy CNCC Screen	On the Discard Policy CNC Console screen, the WARNING level was displayed as blank instead of showing the appropriate warning message. **Doc Impact:** There is no doc impact.	3	24.2.0

Table 4-25 (Cont.) Ingress Gateway 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37114469	Multiple warning messages in CNCC logs	Multiple warning messages were observed in the CNC Console logs. **Doc Impact:** There is no doc impact.	3	22.4.4
35217312	Plaintext HTTP/1.1 attack on N32 IGW leads to high memory consumption	A plaintext HTTP/1.1 attack on the N32 Ingress Gateway caused high memory consumption. **Doc Impact:** There is no doc impact.	3	22.3.1
37333191	Pod Protection using Rate Limiting :- "oc_ingressgateway_http_responses_total" metrics are not updated when call is rejected by ratelimiting	The *oc_ingressgateway_http_responses_total* metric was not updated when a call was rejected due to rate limiting in the Pod Protection feature. **Doc Impact:** There is no doc impact.	3	25.1.100
37369197	Pod Protection using Rate Limiting :- ASM enabled :- Error reason for Pod protection by rate limiting is not updated for default error profile.	When Pod Protection using Rate Limiting was enabled with ASM, the error reason for pod protection by rate limiting was not updated for the default error profile. **Doc Impact:** There is no doc impact.	4	25.1.100
37417212	Pod Protection using Rate Limiting :- ASM enabled : Rest Configuration is success for ERROR Profile which is not defined in values file	When ASM was enabled for Pod Protection using Rate Limiting, the REST configuration for the ERROR profile succeeded despite the profile not being defined in the values file. **Doc Impact:** There is no doc impact.	4	25.1.1000

Table 4-25 (Cont.) Ingress Gateway 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37416293	Pod Protection using Rate Limiting :- ASM enabled : Fill rate is allowing decimal value during helm but same is rejecting in REST configuration	When configuring Pod Protection using Rate Limiting with ASM enabled, the Helm interface allowed you to enter decimal values for the fill rate. **Doc Impact:** There is no doc impact.	4	25.1.1000
36704055	Adding load level as dimension in ingressgateway_route_overloadcontrol_discard metrics	It was difficult to determine the specific load level causing traffic discards due to absence of the load_level dimension in the *ingressgateway_route_overloadcontrol_discard* metric. **Doc Impact:** There is no doc impact.	4	24.2.0
35983660	NRF- Incorrect "detail" value in CCA Header Response when missing mandatory "exp/aud claim" for feature - CCA Header Validation	Ingress Gateway incorrectly populated the "detail" value in the CCA header response when a mandatory "exp/aud claim" was missing, leading to misleading error information. **Doc Impact:** There is no doc impact.	4	23.2.0

Table 4-25 (Cont.) Ingress Gateway 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37756514	Pod-protection :- Congestion Configuration refreshInterval default value showing 5000 instead of 500 and Observed NPE if we configure 50000ms	In the pod protection congestion configuration, the default value for refreshInterval was incorrectly displayed as 5000 milliseconds instead of 500 milliseconds. **Doc Impact:** There is no doc impact.	4	25.1.200
37751980	Pod-protection :- Some of the pod protection for rate limiting metrics are not showing in prometheous	Some pod protection metrics for rate limiting were not displayed in Prometheus due to missing configurations in the monitoring setup. **Doc Impact:** There is no doc impact.	4	25.1.200

> **Note**
>
> Resolved bugs from 24.2.0 have been forward ported to Release 25.1.200.

4.2.12.6 Common Configuration Service Resolved Bugs

Release 25.1.201

There are no resolved bugs in this release.

Release 25.1.200

Table 4-26 Common Configuration Service 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
37563087	Traffic routing done based on deleted peer/ peerset and routes	Traffic was routed based on deleted peer or peer set routes. **Doc Impact:** There is no doc impact.	2	25.1.100

4.2.12.7 Helm Test Resolved Bugs

Release 25.1.200

There are no resolved bugs in this release.

4.2.12.8 App-Info Resolved Bugs

Release 25.1.200

There are no resolved bugs in this release.

4.2.12.9 Mediation Resolved Bugs

Release 25.1.200

Table 4-27 Mediation 25.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37917884	Parsing issue observed in nf-mediation for requestIngress and requestEgress triggerPoints when request payload is null	A parsing issue occurred in nf-mediation for requestIngress and requestEgress triggerPoints when the request payload was null. **Doc Impact:** There is no doc impact.	3	25.1.103
36605719	Warnings being displayed while installing mediation due to k8sResource.container.prefix/suffix parameter	While installing Mediation, a warning appeared due to the presence of the k8sResource.container.prefix/suffix parameter. **Doc Impact:** There is no doc impact.	4	24.1.0

4.2.12.10 NRF-Client Resolved Bugs

Release 25.1.202

Table 4-28 NRF-Client 25.1.202 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
38090009	Nrf Client Discovery and Management Pod showing multiple restarts during uptake of NRF-Client 25.1.201	During the deployment of multiple management Pods associated with the Leader Pod, an error occurred due to discrepancies in the libraries used.	2	25.1.201

Release 25.1.201

Table 4-29 NRF-Client 25.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
38079766	24.2.7 NPE seen in nrf-client-nfmanagement during SM performance run in Policy (24.2.6)	Heart beat process have an special case so we are trying to clean up a given map structure some times it is no created properly, after the fix, we managed correctly and the NPE is not happening.	3	24.2.7
37680409	Upgrading PCF from 23.4.6 to 24.2.4 Leads to -mangement pods stuck in Crashloopback (NRF-client 25.1.200)	Issues while upgrading NRF client from 23.6 to 24.2.x versions	2	24.2.4
37746681	NRF-Client Sends continuous PUT/PATCH requests to NRF when UDR is in SUSPENDED state	When the NF changes from running to not running, NRF-client enters into an endless cycle of PUT and PATCH request part of the heartbeat process. This overloads with many requests.	2	25.1.100
37823559	Upgrade fails from PCF 24.1.0 to 24.2.0 " Error creating bean with name 'hookService' defined in URL" (25.1.200)	While upgrading NRF-client some how there are multiple records in the common config hook db, this generates issues while completing the hook process. Until now the workaround was to manually delete the duplicate records.	2	24.2.0

Release 25.1.200

There are no resolved bugs in this release.

4.2.12.11 Perf-Info Resolved Bugs

Release 25.1.200

There are no resolved bugs in this release.

4.2.12.12 Debug Tool Resolved Bugs

Release 25.1.200

There are no resolved bugs in this release.

4.3 Known Bug List

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

4.3.1 BSF Known Bugs

Release 25.1.200

Table 4-30 BSF 25.1.200 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37977860	APIGW/NRF-Client Error Response Logging configuration gets overwritten when changing log level in CM-Service	The NRF-Client error response enhancements configuration gets overwritten when changing log level in the CM Service.	The NRF-Client's Error Response Enhancements configuration is susceptible to being overwritten when log-level changes are made in the CM-Service. Specifically, when adjusting the log level for NRF-Client, the logSubscriberInfo and additionalErrorLogging configurations are lost, impacting the system's error-handling capabilities. **Workaround:** The system currently allows direct log-level configuration changes by sending requests to the Common Config Server endpoint. For instance, if the configuration for NRF-Client is accidentally overwritten due to log-level adjustments, the following curl command to the CM-Service pod can restore the settings: `kubectl exec -it -n <NAMESPACE> service/<CM-SERVICE-NAME> -- curl -X PUT http://<CM-SERVICE-NAME>:8000/nrf/nf-common-component/v1/nrf-client-nfmanagement/logging -H "Content-Type: application/json" -d '{"appLogLevel":"WARN","packageLogLevel":[{"packageName":"root","logLevelForPackage":"WARN"}],"logSubscriberInfo":"DISABLED","additionalErrorLogging":"DISABLED"}'`	3	25.1.200

4.3.2 CNC Console Known Bugs

Release 25.1.200

There are no known bugs in this release.

4.3.3 cnDBTier Known Bugs

Release 25.1.201

Table 4-31 cnDBTier 25.1.201 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
38199454	DB Entries on Site-1 and Site-2 are not in sync after doing an in service upgrade from PCF 24.2.6 to 25.1.200 on a 2 site GR setup	After performing an in-service upgrade from PCF version 24.2.6 to 25.1.200 on a 2-site Geo-Replication (GR) setup, database entries between Site-1 and Site-2 are not in sync.	Replication delay is observed.	2	24.2.6

Release 25.1.200

Table 4-32 cnDBTier 25.1.200 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37859029	`dbtscale_ndbmtd_pods` failed when ndb backup triggered while scaling in progress	`dbtscale_ndbmtd_pods` failed when ndb backup is triggered while scaling in progress.	Unable to scale the data nodes when backup is in progress. **Workaround**: Perform one of the following workarounds: • Use the `dbtscale_ndbmtd_pods` script from the separate patch included in the cnDBTier scripts package version 25.1.200.0.1. • Follow the manual procedures for scaling the data nodes. • If data nodes are restarting during the re partitioning of the tables, then run the `dbt_reorg_table_partition` script after the restart to ensure all table partitions are reorganized across the data nodes.	2	25.1.100

Table 4-32 (Cont.) cnDBTier 25.1.200 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release

38204306	`dbtremovesite` script exits with ERROR - DBTIER_SCRIPT_VERSION (25.1.100) does not match DBTIER_LIBRARY_VERSION (25.1.200)	The `dbtremovesite` script exits with an error due to a file mismatch issue.	Due to the script failure, site migration may fail.
			Workaround:
			• A separate release of tools folder will be delivered which includes this `dbtremovesite` script.
			• Perform the following steps:
			1. Navigate to the folder `<csar_extract>/Artifacts/Scripts/tools/bin`.
			`cd <csar_extract>/Artifacts/Scripts/tools/bin`
			2. Run the following commands:
			`chmod 755 dbtremovesite`
			`export OCCNE_VERSION=<substitute DBTierversion>`
			`sed -e 's/<\${OCCNE_VERSION}>/'${OCCNE_VERSION}'/' -i dbtremovesite`
				2	25.1.200

37864092	dbtscale_ndbmtd_pods script exited with 'Create Nodegroup FAILED' for wrong nodegroup	In a two site, ASM enabled, backup encrypted and password encrypted setup, the horizontal data pod scaling failed while using the `dbtscale_ndbmtd_pods` script and exited with 'Create Nodegroup FAILED" error.	Scaling of data nodes will not be successful as the new data nodes will still be in the beginning phase. **Workaround**: Perform one of the following workarounds: • Use the `dbtscale_ndbmtd_pods` script from the separate patch included in the cnDBTier scripts package version 25.1.200.0.1. • Follow the manual procedures for scaling the data nodes.	2	25.1.100

Table 4-32 (Cont.) cnDBTier 25.1.200 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
38144181	Add the additional replication error numbers, 1091 and 1826 to the list of replication errors and remove the error number 1094 from the list	Added the following new error numbers to the list of replication errors: • 1091 (Can't DROP – column/key doesn't exist) • 1826 (Duplicate foreign key constraint name) Removed the error "1094 - Unknown command" from the list.	During georeplication process, when the errors 1091 or 1826 occur in the replication channel, the replication fails. **Workaround**: Configure the following replication errors 1091 and 1826 in the `replicationskiperrors.replicationerrornumbers` section of the custom_values.yaml file: • 1091 (Can't DROP – column/key doesn't exist) • 1826 (Duplicate foreign key constraint name) With this, when either of the error occurs, they will be skipped and georeplication process in continued.	3	23.4.2
37859265	`dbtscale_ndbmtd_pods` disrupted by `ndbmtd` pod restart	Schema re-partitioning fails when other data nodes are restarting, requiring the `dbt_reorg_table_partition` script to be re-executed after the restart.	Repartitioning of the tables will fail. **Workaround**: Perform one of the following workarounds: • Use the `dbtscale_ndbmtd_pods` script from the separate patch included in the cnDBTier scripts package version 25.1.200.0.1. • Follow the manual procedures for scaling the data nodes. • If data nodes are restarting during the repartitioning of the tables, then run the `dbt_reorg_table_partition` script after the restart to ensure all table partitions are reorganized across the data nodes.	3	25.1.100
38236749	DR getting stuck for fatal scenario on prefix enabled 4-site single-channel IPv6 setup	Georeplication recovery is stuck if 2 sites are uninstalled in a 4-site scenario and respective IP's are removed from remote site IP	**Workaround**: Perform one of the following workarounds depending upon the Fixed IP's used for the remote site IP: • If fixed IPs are used, then do not remove them from the remote site IP. • If dynamic IPs are used, then any dummy IP can be used for the remote site IP.		

Table 4-32 (Cont.) cnDBTier 25.1.200 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
38199454	DB Entries on Site-1 and Site-2 are not in sync after doing an in service upgrade from PCF 24.2.6 to 25.1.200 on a 2 site GR setup	After performing an in-service upgrade from PCF version 24.2.6 to 25.1.200 on a 2-site georeplication (GR) setup, database entries between Site-1 and Site-2 are not in sync.	Replication delay is observed. **Workaround**: There is no workaround.	2	24.2.6
38220013	`dbtrecover` Script is affecting `db-monitor-svc`.	Intermittently after running georeplication recovery, `db-mon-svc` has deadlock threads. `Db-mon-svc API` and metric scraping are not working until it gets restarted.	**Workaround**: Restart the DB Monitor service after georeplication recovery is completed.	3	25.1.100

4.3.4 CNE Known Bugs

Release 25.1.200

Table 4-33 CNE 25.1.200 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 x9-2 server based BareMetal CNE. • Use CNE 24.3.1 or older version on X9-2 servers.	2	23.4.0
38106756	CNE self upgrade failed due to multus Race condition	When performing CNE upgrade with CNLB-enabled option, upgrade fails intermittently because of a race in Multus that will prevent the pod from starting.	CNE upgrade with CNLB-enabled option fails. There is no impact on LBVM- based deployments. **Workaround**: Run the following command on all the nodes: `sudo rm -R /opt/cni/bin/multus-shim`	3	25.1.200

OSO Known Bugs

Release 25.1.200

There are no known bugs in this release.

4.3.5 NRF Known Bugs

Release 25.1.200

Table 4-34 NRF 25.1.200 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
38327826	Message copy feature: Access token request generated at EGW towards NRF not being sent to kafka properly	There is an issue with the access token request generated at the Egress Gateway. The response message received at the Egress Gateway from the access token microservice is being fed into Kafka, but the request message is not being sent to Kafka. Both the request and response messages need to be fed into the same Kafka partition for the same transaction.	The response message received at Egress Gateway from Access Token microservice is being fed into Kafka, while the request message is not being sent in Kafka. **Workaround**: There is no workaround.	3	25.1.200

Table 4-34 (Cont.) NRF 25.1.200 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37412089	For NFSetId case-sensitive validation, registration request is getting accepted for NID having value not compliant to fixed length of 8 digit hexadecimal number as per 3GPP.	For NFSetId case-sensitive validation, registration request is getting accepted for NID having value not compliant to fixed length of 8 digit hexadecimal number as per 3GPP.	NRF will accept the NFRegister/ NFDiscover service operations request with non-compliant NFSetID containing NID digits. **Workaround:** NFs should use correct length of NID digits as per 3GPP for NFRegister/ NFDiscover service operations request.	3	23.4.6
37760595	Discovery query results in incorrect match with preferred-locality=US%2bEast	NRF is returning NFProfile ordered at first position with locality matching with space (that is, US East) while query contains + (that is, US+East).	NFProfiles in response may be ordered with space first then followed by other localities. **Workaround:** Locality attribute should not have space or plus as special characters. Or if query have %252B as encoded character then NFProfile with + will match that is, US+East.	3	24.2.4

Table 4-34 (Cont.) NRF 25.1.200 Known Bugs

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

Table 4-34 (Cont.) NRF 25.1.200 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37965223	Error Codes are not picked from errorCodeProfile configuration for Pod protection with rate limit	Error Codes are not picked from errorCodeProfile configuration for Pod protection with rate limit.	When Ingress Gateway rejects the requests, it takes the error code from Helm attribute errorCodeProfiles instead of REST. **Workaround:** Update the error code for *ERR_POD_PROTECTION_RATE_LIMIT* in the helm attribute *ingressgateway.errorCodeProfiles.*	3	25.1.200
37965589	The Ingress gateway pod restarted and went into crashloopbackoff when 10k traffic was sent to a single pod	The Ingress gateway pod restarted and went into crashloopbackoff when 10k traffic was sent to a single pod.	The ingress gateway Pod Protection using rate limiting feature was enabled. To simulate high burst of traffic, 10k TPS was sent to a single IGW pod. The Ingress Gateway pod restarted and the pod went into crashloopbackoff state. The issue is observed with ASM enabled. The side car container crashed due to OOM. **Workaround:** Traffic cannot reach to 10k.	3	25.1.200

Table 4-34 (Cont.) NRF 25.1.200 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37604778	TLS1.3 Handshake is failing between NRF and SCP	TLS1.3 Handshake is failing between NRF and SCP as SCP was sending Session resumption extensions towards NRF (Ingress Gateway).	TLS v1.3 will not work if Client is sending session resumption extensions. **Workaround:** Client should not send Session Resumption extension.	3	24.2.3
38104210	NFUpdate - Partial update dnnUpfInfoList and dnnSmfInfoList are accepting string value instead of object	NFUpdate - Partial update dnnUpfInfoList and dnnSmfInfoList are accepting string value instead of object	*dnnUpfInfoList* and *dnnSmfInfoList* will have wrong information as per 3GPP. This is fault insertion case, when string values are used instead of the *DnnSmfInfoItem* and *DnnUpfInfoItem* object. **Workaround:** *dnnSmfInfoItem* and d*nnUpfInfoItem* attributes shall be used as per 3GPP during patch to avoid this issue.	3	25.1.100

Table 4-34 (Cont.) NRF 25.1.200 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37412138	Error response generated by NRF needs to be corrected when registration request is sent with incorrect order for mcc and mnc	Error response generated by NRF needs to be corrected when registration request is sent with incorrect order for mcc and mnc.	No Impact on signaling message processing. Only error message details doesn't include correct error reason. **Workaround:** There is no workaround available.	4	23.4.6
38103938	log4j2_events_total metric is not getting pegged	*log4j2_events_total* metric is not getting pegged.	Metric for log4j is not pegged. **Workaround:** There is no workaround available.	4	25.1.200
38103958	Congestion Config CNC Console GUI screen not working correctly	Congestion Config CNC Console GUI screen not working correctly.	CNC Console GUI is not working for congestion config. **Workaround:** There is no workaround available.	4	25.1.200

4.3.6 NSSF Known Bugs

Release 25.1.200

Table 4-35 NSSF 25.1.200 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37048499	GR replication is breaking post rollback to of CNDB 24.2.1-rc.4	The cnDBTier replication mechanism is experiencing performance degradation during rollbacks under high transaction volumes, leading to potential transaction ordering inconsistencies and constraint failures on the secondary site. Additionally, any binlog instruction failure is disrupting the replication channel. For the Network Service Selection Function (NSSF), the NsAvailability functionality is encountering a replication channel break when rolling back an upgrade from 24.2.x to 24.3.x if an availability delete and an availability update are occurring within a few seconds.	During the rollback of an upgrade from 24.2.x to 24.3.x, the Network Service Selection Function's (NSSF) Availability functionality may experience a replication channel break. This can occur when an availability delete and an availability update happen within a short time frame of a couple of seconds. As a result, the replication channel may be disrupted. **Workaround:** To recover the replication channel, follow these steps: • See the "Resolving Georeplication Failure Between cnDBTierTier Clusters in a Two Site Replication" section in *Oracle Communications Cloud Native Core, cnDBTierTier Installation,*	24.3.0	2

Table 4-35 (Cont.) NSSF 25.1.200 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
			Upgrade, and Fault Recovery Guide. • Follow the replication channel recovery procedure as described in the guide.		
37763453	Error code 500, instead 4XX, when NSSF receives duplicated incorrect Authorization	When the NSSF receives a request with a duplicated and incorrect Authorization header, it returns an HTTP 500 Internal Server Error instead of the expected 4XX error.	When an incorrect authentication token is provided, the Internet Gateway (IGW) does not respond with an error message. However, there is no loss of traffic. **Workaround:** There is no workaround.	3	24.3.0
37762864	[10.5K TPS] nrf-client discovery and management pod has restarted when all cnDBTier pod faults using chaos-mesh	When all cnDBTier pods are subjected to a pod fault using chaos-mesh, the nrf-client discovery and management pod unexpectedly restarts. This issue occurs in a specific test environment with distributed traffic and replication channel configurations.	When the Cloud Native Database (cnDBTier) is forcefully kept in a stuck state, the Network Repository Function (NRF) client pods may enter a state of continuous restart. However, there is no impact on traffic once the cnDBTier pods recover. **Workaround:** There is no workaround.	3	25.1.200

Table 4-35 (Cont.) NSSF 25.1.200 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37731732	Autopopulation with 3NRFs: Even though candidate AMF doesn't have same plmn as amfset it is storing in database and is getting resolved when amf resolution is called	During AMF resolution, the system includes candidate AMFs with different PLMNs in the AMF set, even though they should only include AMFs with the same PLMN.	When the Cloud Native Database (cnDBTier) is forcefully kept in a stuck state, the Network Repository Function (NRF) client pods may enter a state of continuous restart. However, there is no impact on traffic once the cnDBTier pods recover. **Workaround:** There is no workaround.	3	25.1.200
37684563	[10.5K Traffic—without Replication Break] While 7K burst traffic to site1, NSSF reduced the success rate by 3.528% with 500 and 503 error code and then recovered it	When transferring traffic from Site2 and Site3 to Site1, the NSSF experiences a temporary drop in success rate by 3.528%, with 500 and 503 error codes.	When traffic is moved from one site to another, there may be an intermittent loss of traffic. The impact is minimal, resulting in approximately 3.5% of traffic loss for a few seconds, after which the traffic recovers. **Workaround:** There is no workaround.	3	25.1.200
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 adding an empty frame to all ns-selection and ns-availability requests, the NSSF rejects a small percentage of traffic (0.045%) with a 503 error code. This issue occurs during high traffic loads.	There is minimal impact on traffic, resulting in approximately 3.5% of traffic loss for a few seconds, after which the traffic recovers. **Workaround:** There is no workaround.	3	25.1.200

Table 4-35 (Cont.) NSSF 25.1.200 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37639879	oauth failure is not coming in oc_ingressgateway_http_responses_total metrics	The oauth failure is not coming in oc_ingressgateway_http_responses_total metrics but it seen in the oc_oauth_validation_failure_total metric.	There is no impact on traffic. **Workaround:** There is no workaround.	3	25.1.200
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.	When an invalid Accept header is provided, the NSSF responds with 500 status codes for nssai-auth PUT and DELETE requests instead of sending 4xx responses as expected. This issue leads to incorrect database operations and unnecessary notifications to the AMF.	There is no impact on traffic. **Workaround:** There is no workaround.	3	25.1.200
37606284	With DNS SRV feature enabled for selection of NRF, NSSF fails to establish connection with NRF	When an invalid Accept header is provided in requests to the NSSF, it incorrectly sends a 500 response for PUT operations and a 204 response for DELETE operations on the `nsssai-auth` configuration. Instead, it should send a 4xx response without performing any database operations or triggering notifications to the AMF.	There is no impact on traffic. **Workaround:** There is no workaround.	3	25.1.200

Table 4-35 (Cont.) NSSF 25.1.200 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
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.	NSSF sends success responses for PDU session establishment requests targeting an unconfigured slice (0.4% of 1K TPS traffic) while sending failure responses (403 and 503) for requests targeting valid, configured slices (9K TPS traffic). This issue occurs during PDU session establishment, despite initial registration, UE configuration, and handover selection working correctly for invalid slices.	There is minimal impact on traffic. **Workaround:** There is no workaround.	3	24.3.0

Table 4-35 (Cont.) NSSF 25.1.200 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37184196	3-site GR setup ASM and Oauth Enabled : 10.5K TPS Traffic on SITE1 : during restoration of site (post Failover for 18 hours), new NsAvailability PUT is not syncing to site which is recovered	In a 3-site setup with ASM and OAuth enabled, during the restoration of a site after an 18-hour failover, the NsAvailability PUT request for a specific slice is not syncing to the recovered site. This occurs when 10.5K TPS traffic is running on the remaining active site (SITE-1), and the replication channels are restored. As a result, Ns-Selection for the slice on the recovered site (SITE-2) fails, even though Ns-Selection on the active site (SITE-1) is successful.	There is minimal impact on traffic. **Workaround:** There is no workaround.	3	24.3.0
37136539	[dnsSrvEnabled: false] [peer Health monitoring: disabled] NSSF is not sending the notification towards peer2 host if peer1 is down	NSSF fails to send notifications to the peer2 host when peer1 is down, and both dnsSrvEnabled and peer monitoring are disabled. In the provided configuration, the host nssf-scp-3-scp-worker.ocnssf-scp-3 (peer1) is down, but the egress gateway does not route notifications to the peer2 host as expected.	There is a loss of notification message in a specific corner case when static routing is being used. **Workaround:** Enable dnsSrv and use virtual FQDNs.	3	24.2.1

Table 4-35 (Cont.) NSSF 25.1.200 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37136248	If dnsSrvEnabled is set to false and peer1 is used as a virtual host, the egress gateway will not sending the notifcation to peer2 host and peer health status is empty	When `dnsSrvEnabled` is set to **false** and `peer1` is configured as a virtual host, the egress gateway fails to send notifications to the `peer2` host. As a result, the peer health status remains empty. Wireshark analysis reveals a 400 Bad Request error for the notification attempt.	There is no impact on traffic, as with retrial, the message gets to the correct node. **Workaround:** There is no workaround.	3	24.2.1
37099843	Upgrade 3 Site GR Setup, while upgrading NSSF and cnDBTier, we observed that the Ns-availability success rate dropped 0.07%, 0.77%, and 1.19%, respectively, for each site, and we got 500, 503, and 403, 408 error codes.	During the upgrade process of a 3-Site GR Setup, the Ns-availability success rate experiences a drop of 0.07%, 0.77%, and 1.19% for each site, respectively, when upgrading NSSF and cnDBTier. This issue is accompanied by error codes 500, 503, 403, and 408.	There is minimal impact on traffic during upgrade, resulting in approximately 0.25 to 1% of messages being lost. **Workaround:** There is no workaround.	3	24.3.0

Table 4-35 (Cont.) NSSF 25.1.200 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36734417	NSSF 2 Site GR :IN service solution Upgrade : 1.25K TPS : traffic loss of 0.259% and 0.027% at Site 1 and Site 2 during the NSSF upgrades, with latency of roughly 1.43 seconds and 886 ms.	During the upgrade process of a 2-Site GR Setup, traffic loss is observed at Site 1 and Site 2, with a loss of 0.259% and 0.027%, respectively. This is accompanied by increased latency, reaching 1.43 seconds at Site 1 and 886 milliseconds at Site 2. The issue occurs while upgrading NSSF.	There is minimal impact on traffic during upgrade, resulting in approximately 0.25% of messages being lost. **Workaround:** There is no workaround.	3	24.2.0
36662054	NSSF-CNCC: Ingress pod: Discard Policy mapping configured without mandatory param	The CNCC GUI is experiencing an issue where the Discard Policy mapping can be configured without mandatory parameters. This is due to a lack of validation checks, allowing users to save the mapping without providing essential information.	There is no impact on traffic. **Workaround:** The operator can configure with proper values.	3	24.1.0

Table 4-35 (Cont.) NSSF 25.1.200 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.	NSSF is not properly validating certain parameters in the oauthvalidator configuration, specifically KeyId, certName, kSecretName, and certAlgorithm. Invalid values for these fields are being accepted without triggering an error or validation message.	There is no impact on traffic. **Workaround:** While configuring OAuth validator configuration, the operator needs to use proper values.	3	24.1.0
36285762	After restarting the NSselection pod, NSSF is transmitting an inaccurate NF Level value to ZERO percentage.	After restarting the NSselection pod, the NSSF system is incorrectly reporting an NF Level value of zero percent. This issue is observed when retrieving the NSselection request for EPS to 5G selection, and it results in the absence of ocnssf-selection data in the response. The system should accurately reflect the NF Level, especially when there is load information available.	There is no impact on traffic. **Workaround:** There is no workaround.	3	23.4.0

Table 4-35 (Cont.) NSSF 25.1.200 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36265745	NSSF is only sending NF-Instanse/NF-Service load level information for multiple AMF Get Requests	The NSSF system is inconsistently providing NF-Instance and NF-Service load level information in response to AMF Get Requests. In some cases, only the NF-Instance load level is sent, while in others, only the NF-Service load level is included.	There is no impact on traffic. **Workaround:** There is no workaround.	3	23.4.0
35971708	while pod protection is disabled, OcnssfIngressGatewayPodResourceStateMajor alert is not clear and resource metric is not updating to -1	When disabling pod protection, the system fails to update the resource metric to -1 and does not clear the `OcnssfIngressGatewayPodResourceStateMajor` alert. This results in an incorrect view, as the congestion alert is cleared, but the resource alerts remain visible. The issue suggests a potential problem with the system's ability to accurately reflect resource-related changes.	There is no impact on traffic. **Workaround:** There is no workaround.	3	23.3.0

Table 4-35 (Cont.) NSSF 25.1.200 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35922130	Key Validation is missing for IGW pod protection parameter name configuration	The system is not correctly processing certain keys in the provided curl commands. Specifically, the keys 'actionSampling Period', 'name', 'cpu', and 'pendingMessag e' are not being handled as expected	There is no impact on traffic. **Workaround:** Configure NSSF with proper values as per the *Oracle Communications Cloud Native Core, Network Slice Selection Function REST Specification Guide*.	3	23.3.0
35921656	NSSF should validate the integer pod protection parameter limit.	The system is not properly validating integer parameters in the provided curl commands. Specifically, the parameters 'monitoringInterv al', 'stateChangeSa mpleCount', 'actionSampling Period', and 'incrementBy' are not being checked for valid values.	There is no impact on traffic. **Workaround:** The operator can configure and make sure the values configured must be as per *Oracle Communications Cloud Native Core, Network Slice Selection Function REST Specification Guide*.	3	23.3.0

Table 4-35 (Cont.) NSSF 25.1.200 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35888411	Wrong peer health status is coming "DNS SRV Based Selection of SCP in NSSF"	When peer monitoring is enabled and dnsSrvEnabled is disabled, the system displays incorrect peer health status. With an invalid SCP IP configured as a host and a virtual host with valid data, the health status shows the invalid SCP as healthy, which is incorrect. The health status for the peer configured via the virtual host is missing and should also be indicated as unhealthy.	There is no impact on traffic flow, as a non-responsive SCP is not being considered for status. **Workaround:** There is no workaround.	3	23.3.0
35860137	In Policy Mapping Configuration in Ingress Gateway, For the samplingPeriod parameter, max value of parameter validation should be necessary.	In the Policy Mapping Configuration of the Ingress Gateway, the maximum value for the samplingPeriod parameter is not being validated correctly. When a user sets an extremely high value for this parameter, the system accepts it without any error or validation.	There is no impact on traffic flow. **Workaround:** There is no workaround.	3	23.3.0

Table 4-35 (Cont.) NSSF 25.1.200 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37622760	NSSF should send 415 responses to ns-selection and ns-availability requests if their content type is invalid.	NSSF is not responding with the correct error code when receiving ns-selection and ns-availability requests with invalid content types. Instead of sending a 415 response as per the 3GPP specification, it returns a 500 error with an "UNSPECIFIED_NF_FAILURE" message.	There is no impact on traffic flow. **Workaround:** There is no workaround.	4	25.1.200
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 ns-selection and ns-availability requests are made with an invalid Accept header, the NSSF responds with a 404 error instead of the expected 500 error with the detail "No acceptable representation." This behavior is observed for both subscription deletion and patch requests.	There is no impact on traffic flow. **Workaround:** There is no workaround.	4	25.1.200

Table 4-35 (Cont.) NSSF 25.1.200 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37612743	If URLs for ns-selection and ns-availability are invalid, NSSF should return a 400 error code and title with INVALID_URI.	When ns-selection and ns-availability requests are made with invalid URLs, the NSSF responds with a 404 error instead of the expected 400 error with the title "INVALID_URI." This issue is observed across various call flows, including UE Config, Subscription POST, Ns-Availability DELETE, unsubscription, Subscription Patch, and Availability PATCH.	There is no impact on traffic flow. **Workaround:** There is no workaround.	4	25.1.200
37606772	3-site GR setup ASM and Oauth Enabled: 15K TPS Traffic on SITE1 : we observed the 503 SERVICE_UNAVAILABLE error code	In a 3-site GR setup with ASM and OAuth enabled, when traffic is distributed across three NSSF instances and replication channels are brought down, the NSSF starts rejecting some traffic with a 503 "SERVICE_UNAVAILABLE" error code as the traffic load increases.	There is minimal impact on traffic in an overload scenario. **Workaround:** There is no workaround.	4	25.1.200

Table 4-35 (Cont.) NSSF 25.1.200 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37592343	Subscription Patch should be a part of Availability Sub Success (2xx) % panel in Grafana Dashboard	The Grafana dashboard's Availability Sub Success (2xx) % panel does not include subscription patch requests. When the SUMOD feature is disabled in the NSSF ocnssf_custom_values.yaml file, subscription patch requests fail with a 405 error, and this information should be reflected in the dashboard to provide a comprehensive view of subscription success rates.	There is no impact on traffic. **Workaround:** There is no workaround.	4	25.1.200
36881883	In Grafana, Service Status Panel is showing more than 100% for Ns-Selection and Ns-Avaliability Data	The Service Status Panel in Grafana shows more than 100% for NS selection and availability data.	There is no service impact. **Workaround:** There is no workaround.	4	24.2.0
36653494	If KID is missing in access token, NSSF should not send "Kid missing" instead of "kid configured does not match with the one present in the token"	When the KID is missing in the access token, NSSF sends "kid configured does not match with the one present in the token" instead of indicating that the KID is missing.	There is no impact on traffic, as the error code is proper. **Workaround:** There is no workaround.	4	24.1.0

Table 4-35 (Cont.) NSSF 25.1.200 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35986423	Both IGW pod protection and overload feature enabled, NSSF is not clearing the overload alerts when overload feature disabled in runtime.	NSSF does not clear overload alerts when the overload feature is disabled at runtime, even though IGW pod protection and overload feature were initially enabled.	There is no impact on traffic. **Workaround:** There is no workaround.	4	23.3.0
35986361	NSSF will not modify the weight values in metrics simultaneously if the weight value changes. The weight metric has changed when any pod raises a new alarm.	NSSF does not update the weight values in metrics simultaneously when the weight value changes, instead, the weight metric is updated only when a new alarm is raised.	There is no impact on traffic, as NSSF takes care of the condition, but the alert is subsided only when there is a change in state. **Workaround:** There is no workaround.	4	23.3.0
35855377	The abatementValue less than onsetValue should be validated by NSSF in the Overload Level Threshold Configuration.	NSSF does not validate that the abatement value is less than the onset value in the Overload Level Threshold Configuration, allowing invalid configurations to be successfully applied.	There is no impact on traffic. **Workaround:** Configure NSSF with proper values as per *Oracle Communications Cloud Native Core, Network Slice Selection Function REST Specification Guide*.	4	23.3.0

4.3.7 OCCM Known Bugs

Release 25.1.200

There are no known bugs in this release.

4.3.8 Policy Known Bugs

Table 4-36 Policy 25.1.200 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37870899	Policy upgrade to 25.1.200 from 24.2.5, CHF notification failed with error code 500, DB Error 1054 "Unknown column 'p1_0.mode' in 'field list'"	While upgrading Policy from 24.2.5 to 25.1.200, CHF notification fails with error code 500, DB Error 1054 "Unknown column 'p1_0.mode' in 'field list'".	If you are upgrading cnDBTier to a version that does not have the fix, there can be a schema synchronization issue between the sites. This can result in the replication link failure in certain conditions. **Workaround**: cnDBTier 24.2.6 release is a pre-requisite for upgrading to Policy 25.1.200.	2	25.1.200
37952431	Egress traffic getting increased while the connectivity to ARS pods is down causing traffic discards	Traffic at Egress Gateway increased while the connectivity to ARS pods is down, causing traffic discards.	In a high performance setup, restarting two or all of the three ARS pods can lead to traffic build up at Egress Gateway. This can result in increased egress traffic and can also make few requests getting timed out. **Workaround**: There is no workaround if multiple ARS pods are restarted. ARS service can be deployed with at most 3 pods (or as recommended by the Oracle engineering team). In such a case, if one or few of the pods restart, the remaining pods can handle the traffic.	2	25.1.200

Table 4-36 (Cont.) Policy 25.1.200 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36832070	Issue with "Enforcement Network Element Name" blockly.	The "Enforcement Network Element Name" blockly is frequently causing the Policy Rule Engine (PRE) to halt its evaluation of the policy tree when encountered.	There is no signalling failure. But, randomly some of the sessions are responded to with success without charging rule. **Workaround**: There is no workaround available.	3	23.2.8
36913031	pcrf-core calls latency increases in seconds when bulwark locking mechanism is integrated with the Gx interface	Latency for PCRF Core calls increases in seconds when Bulwark locking mechanism is integrated with the Gx interface.	Latency for PCRF Core calls runs into seconds when integrated with Bulwark service. **Workaround**: There is no workaround available.	3	24.2.0
37013029	Missing logs due to "Rejected by OpenSearch" error	Open Search cannot not display the logs that result in parse error. When Buffer Overflow error appears, Open Search fails to display any log.	Open Search cannot display the logs that result in parse error. When Buffer Overflow error appears, open search fails to display any logs. **Workaround**: There is no workaround available.	3	23.4.3
36988075	After PCF pods restart one by one, occasionally it was observed that the PCF performs duplicate subscription on NRF for peer NF.	After the PCF pods restart one by one, occasionally it is observed that the PCF duplicates subscription on NRF for peer NFs.	Due to duplicate subscription and multiple notifications received from NRF, PCF cannot handle NF profile updates. **Workaround**: Enable duplicate subscription feature on NRF, if Oracle NRF is used.	3	24.2.0

Table 4-36 (Cont.) Policy 25.1.200 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
18529357	Missing '3gpp-sbi-correlation-info' header in NRF discovery request from PCF via Egress Gateway, when 3gpp-sbi-correlation-info feature flag enabled in General setting and all linked communication profiles for all interfaces	The '3gpp-sbi-correlation-info' header is missing in NRF discovery request that PCF sent through Egress Gateway, when 3gpp-sbi-correlation-info feature is flag enabled in General setting and there are linked communication profiles for all interfaces.	The header (**3gpp-sbi-correlation-info**) is not propagated to external services (such as NRF) and cannot correlate the requests/calls. **Workaround**: There is no workaround available.	3	25.1.200
38105323	diam-connector pod restart observed.	Diameter Connector pod restarts unexpectedly.	The Diameter Connector can restart due to OOM when burst of Timeouts happen between Diameter Connector and Diameter Gateway due to connection loss or when the service is not reachable. **Workaround:** Enable congestion control for the Diameter Connector.	3	25.1.200

Table 4-36 (Cont.) Policy 25.1.200 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37798499	[AM Performance] disconnecting AMF simulator from Egress for 25Min leads to UE pods restart and Traffic Stuck	When AMF simulator is disconnected from Egress Gateway for 25 minutes or longer, UE pods restart with increased traffic congestion.	UE service pod restarts under the following conditions: • There is a complete outage where complete AMF NF Set is down. • High TPS traffic is running around 40K TPS. • This outage condition remains for more than 25 minutes. The simulation setup used a stubbed AMF (AMF-SIM) that does not fully reflect the real-world behaviour. The scenario assumed 100% failure across the AMF Set by scaling down all the pods (but not the service). This situation does not simulate the realistic network failure. As a result, retry and fallback logic (session retry, discovery refresh, etc.) are not effectively triggered or tested. Additionally, the simulator handling N1N2 messages did not align with how the production AMFs behave, particularly around suspended state detection and discovery behaviour. Complete outage on AMF is not expected. **Workaround:** PCF Session Retry logic can discover the working AMF and redirect the messages.	3	24.2.4

Table 4-36 (Cont.) Policy 25.1.200 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37762722	When PCF is in complete shutdown state, Audit notifications continue to be sent out.	Audit notifications are sent when PCF is in complete shutdown state.	Audit service continues to generate and send Audit Notifications even if the system is in COMPLETE_SHUTDOWN state. **Workaround:** When PCF is in COMPLETE_SHUTDOWN state, Audit service must be manually interrupted using Audit Pause operation in CNC Console.	3	23.2.0
37099406	Error "Got temporary error 245 'Too many active scans, increase MaxNoOfConcurrentScans' from NDBCLUSTER" observed on Binding, while running 43K new call model.	While running 43K new call model, "Got temporary error 245 'Too many active scans, increase MaxNoOfConcurrentScans' from NDBCLUSTER" error is observed in Binding service.	The “Too many active scans, increase MaxNoOfConcurrentScans” error indicates that the database is handling more simultaneous scan operations than it can efficiently process. This issue affects all the services relying on the database. **Workaround**: There is no workaround available.	3	24.2.1
38164639	When rejected UPSIs are retransmitted, old N1 Context is not updated with new PTI	When rejected UPSIs are retransmitted, the old N1 Context is not updated with new PTI.	This happens only when N1 Notify Reject is configured to retransmit the rejected UPSIs. It is a very rare case when a policy is written to send a different UPSI, where new PTI is generated. System Impact depends on UE implementations whether it undoes the previous PTIs associated with policy installation. Otherwise, there is no functional impact. **Workaround**: There is no workaround available.	3	25.1.100

Table 4-36 (Cont.) Policy 25.1.200 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
38167780	Observing that PDS is returning 200 response code with non-null SpendingLimit status in revalidation scenario, instead of 206 response with null Spending Limit status, on receiving error from CHF.	PDS returns 200 response code with non-null SpendingLimit status in revalidation scenario, instead of 206 response with null Spending Limit status, on receiving error from CHF.	When synchronous CHF/OCS integration is configured, a revalidation scenario can result in incorrect handling of a 404 response from CHF by PDS. Specifically, PDS returns a 200 response instead of a 206 response with a non-null Spending Limit status in the body. As a result, SM service receives an incorrect response. SM service fails to delete the dsTypes for Spending Limit from its stored dsTypes, potentially leading to inconsistencies in the system such as Outdated Spending Limit Data and Incorrect Policy Enforcement. **Workaround:** Configure PRE policies to rely solely on the *user.request.ocsSpendingLimitStatus.lastErrorCode* value and ignore the *responseCode*. In such a case, even though an error response is sent to PRE, the impact of this issue can be minimal or negligible, as the PRE evaluation is based on the lastErrorCode value.	3	25.1.200

Table 4-36 (Cont.) Policy 25.1.200 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
38167799	OclogId is not getting added for cleanup flow, when deleting using Session viewer for any service.	When OclogId is deleted using Session Viewer, the OclogId is not getting added to the clean up flow.	Even if this bug does not represent a service malfunction and is not a full impediment to debugging tasks, Log Correlation on query service makes debugging easier in general. **Workaround:** The Query service flows can still be identified on logs without ocLogId. The Query service flows can be identified not only through tools like Wireshark, but also by reading the logs. As Query service flows are usually triggered either manually or using test suites like ATS (except for BSF audit flow that is already being covered by Log Correlation) it is not an impediment to debug.	3	25.1.200
38167812	URI, method, and associationId are not properly logged in Enhanced error response logging for smf update notify and terminate notify	URI, method, and associationId are not properly logged in Enhanced error response logging for SMF Update Notify and Terminate Notify requests.	Unable to see what URI is called when the call fails. **Workaround**: There is no workaround available.	3	25.1.200
38167861	UE Policy service is not triggering second Update Notify request when the first Update Notify fails for same policy actions	UE Policy service does not trigger the 2nd Update Notify request when the first Update Notify fails for same policy actions.	Observe the behaviour of reverting PRA and Policy triggers in case update notify fails. Analyse all the scenarios as AAR-U and STR requests. **Workaround**: There is no workaround available.	3	25.1.200

Table 4-36 (Cont.) Policy 25.1.200 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
38170694	Diam-Gateway reports "Diameter: Error processing message AAR" with DIAMETER_UNABLE_TO_COMPLY (5012) due to improper event handling in its Finite State Machine leading to rejection of signaling messages	The Diam-Gateway is experiencing issues with processing AAR messages due to an error in its internal state management system. This results in the rejection of signaling messages, with the error message "Diameter: Error processing message AAR" and the error code *DIAMETER_UNABLE_TO_COMPLY (5012)*. The error occurs with a frequency of 4 to 5 times within a 6 to 7-minute window during the initial stages of operation and stops once the system load is complete.	You may experience temporary failures in establishing secondary (Rx) sessions during periods of high network load. This issue can cause disruptions in your service, especially at the beginning of the load, until the system stabilizes after a few minutes. **Workaround**: There is no workaround available.	3	25.1.200

Table 4-36 (Cont.) Policy 25.1.200 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
38170881	Policy-ds service pre/post upgrade taking longer time to comeup when upgrading from 24.2.5 to 25.1.200-rc.1	The Policy-ds service is experiencing prolonged startup times when upgrading from version 24.2.5 to 25.1.200. The process is taking longer than expected, both before and after the upgrade is initiated.	The upgrade process from version 24.2.5 to 25.1.200 may result in a longer wait time for the PolicyDS pre-upgrade and post-upgrade tasks to finish. **Workaround**: There is no workaround available.	3	25.1.200
38173953	SSLHandshakeException is seen in TLSv1.3 Connection Between ocamf and Ingress Gateway	An SSLHandshakeException error is occurring in the TLSv1.3 connection between the ocamf and the Ingress Gateway. This exception is causing issues with the secure communication between these two components.	You may encounter failures in UE test cases when triggering TLS 1.3 ATS due to a limitation in the amf simulator tool's handling of TLS v1.3. **Workaround**: There is no workaround available.	3	25.1.200

4.3.9 SCP Known Bugs

SCP 25.1.201 Known Bugs

There are no new known bugs in this release. Known bugs from 25.1.200 have been forward ported to release 25.1.201.

Release 25.1.200

Table 4-37 SCP 25.1.200 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
38154297	trafficFeed_attempted_total metric in SCP is intermittently pegged with an unknown value for the NFServiceType dimension during Notification RxRequest	During a pipeline run on a freeway setup, the trafficfeed_attempted_total metric was observed to be consistently pegged with the NFServiceType value set to "unknown" intermittently.	It has a minor observability impact due to the dimension service type being NA in the metric for a few requests. **Workaround:** None	3	25.1.200
38152282	Certificate Reload Issue in netty context after patching	The SslProviderObject caused a NullPointerException during certificate reload in the Netty context, leading to a failure in context reload.	The certificates will not be updated for downstream connections on certificate reload. **Workaround:** Restart the SCP-Worker pod.	3	25.1.200
38112967	"ocscp_authority" dimension missing in "ocscp_metric_http_rx_res_total" metric	The `ocscp_authority` dimension is missing from the following metrics: • ocscp_metric_http_tx_req_total • ocscp_metric_http_rx_req_total • ocscp_metric_http_tx_res_total • ocscp_metric_http_rx_res_total	It has a minor observability impact due to a dimension invisible in one of the metrics. **Workaround:** None	3	24.3.0
38071919	Port is not derived from NFProfileLevelAttrConfig in case of ModelD Notification and SCP does AR using hardcoded port 80	When a Model-D notification is received, the port is not correctly derived from NFProfileLevelAttrConfig, resulting in SCP using a hard-coded port 80 for alternate routing.	The default port 80 is used irrespective of scheme for notification routing. Also, the port and scheme for the profile level FQDN or IP are not considered. The impact is limited to routing of non-default notification messages as part of Model-D. **Workaround:** None	3	25.1.200
38008367	Overlapping regex validation missing for apiSpecificResourceUri in routing config API	The routing configuration REST API allows overlapping regex patterns in the `apiSpecificResourceUri` field, leading to ambiguous routing when a request matches multiple patterns.	There is conflicting routing config set selection in case of overlapping regex in `apiSpecificResourceUri`. **Workaround:** Overlapping regex should not be configured.	3	25.1.100
37995299	SCP not able to delete foreign SCP routing details post deregistration	When a foreign SCP profile is unregistered, SCP fails to remove the associated routing details for certain profiles.	Some foreign SCP routing rules are not cleared if nfsetId is updated. **Workaround:** None	3	25.1.200

Table 4-37 (Cont.) SCP 25.1.200 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37970295	Worker pod restart observed due to coherence timeout when single cache pod is used	When increasing the number of worker pods from 1 to 23 with only one cache pod in use, worker pods restart due to coherence timeout.	It does not have any impact as SCP redeployment is required to update `nfsetid` and not a recommended change. **Workaround:** None	3	25.1.200
37969345	topologysourceinfo REST API is not case sensitive for nfType	When updating the Topology Source of an NF Type from LOCAL to NRF using the PUT method, the REST API successfully processes the request without errors, but SCP triggers an on-demand audit with `nfType=udm`, resulting in empty NF responses.	The REST API with a case not matching the 3GPP specified NFType would result in an empty response. **Workaround:** Provide `NFType` as per the 3GPP standard.	3	23.4.0
37951970	Unable to edit services of the Registered NF's even if TSI is changed to Local	The services of the registered NFs cannot be edited even if Topology Source Information (TSI) is changed to `Local`.	The services of the registered NFs cannot be edited after Topology Source Information (TSI) is changed to Local. **Workaround:** Profiles can be deleted, and then updated profiles can be added.	3	25.1.200
37949191	ocscp_metric_nf_lci_tx_total metric is incrementing even when no LCI headers are received from peer NFs	The `ocscp_metric_nf_lci_tx_total` metric incorrectly increments even when no LCI headers are received from peer NFs.	It has a minor observability impact. **Workaround:** None	3	25.1.200
37887650	Crash observed on SCP-Worker with traffic feed enabled with 2 trigger points when Traffic exceeds 7K req/sec	When traffic feed is enabled with two trigger points, the SCP-Worker crashes if traffic exceeds 7K requests per second.	The SCP-Worker pod restarts when the traffic feed requests are overloaded. **Workaround:** Traffic is redistributed to other pods.	3	25.1.200
37622431	Audit failures observed during overload situation when traffic is operating at maximum rated capacity and surpasses the pod limits by 50%.	When traffic is operating at maximum rated capacity and exceeds the pod limits by 50%, audit failures are observed while SCP is in the overload condition.	In overload conditions, SCP-Worker pod protection mechanism discards some of the internally generated NRF audit requests. **Workaround:** Audit is periodic in nature and eventually successful when the overload condition subsides.	3	25.1.100
37575057	Duplicate Routing when producer responses with location header in 3xx cases	SCP performs duplicate routing when the producer NF responds with the location header in 3xx cases.	SCP will send requests to producer NF again if the producer NF in redirect URL and alternate routing rules are the same. **Workaround:** None	3	25.1.100

Table 4-37 (Cont.) SCP 25.1.200 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36757321	Observed 429's due to pod overload discards during upgrade from 24.1.0 to 24.2.0-rc.5	During an upgrade from SCP 24.1.0 to 24.2.0, five worker nodes consumed more than six vCPUs while handling 60K MPS, resulting in the generation of 429 errors.	Some discards might be observed during an upgrade in case of bursty traffic due to the SCP-Worker pod protection mechanism. **Workaround:** It is recommended to perform an upgrade during low traffic rate to avoid pod overload.	3	24.2.0
36600245	SCPIgnoreUnknownService Alerts is not getting raised for all the ignored services at SCP	The SCPIgnoreUnknownService alert is not raised for all ignored services, with only the first ignored service triggering an alert.	An alert will not be raised for the first occurrence of an unknown service. **Workaround:** The INFO alert is raised from the second occurrence onward with minimal impact.	3	24.2.0
38188009	In case of scale down of NRF proxy/ mediation pods, scp-worker map keep sending message to old IP Address of already deleted nrfproxy pod.	SCP-Worker keeps sending messages to old IP addresses of already removed `nrfproxy` or mediation pods.	Some inter-microservices requests might be impacted if sent to stale destinations. **Workaround:** Restart SCP-Worker or other pod that displays this behavior where it's unable to establish any connection with other services so that the discovery of target service pods can be refreshed.	3	25.1.200
38098107	SCP is Not considering Version and Trailer fields from Jetty response	SCP is not considering version and trailer fields from Jetty responses.	It does not have any impact as fields are not currently used. **Workaround:** None	4	25.1.200
38088638	Unexpected Increment in ocscp_metric_req_nf_unhealthy_total Metric During producer marked as OD in DS setup	When AUSF is marked as an outlier after receiving 10 messages from SCP, the `ocscp_metric_req_nf_unhealthy_total` metric is incorrectly incremented three times instead of the expected two times.	It has a minor observability impact. **Workaround:** None	4	25.1.200
38079614	SCP All Services: Remove use of java.util.date and org.joda.time. Use java.time instead because of threadsafety and better method list..	SCP services relies on `java.util.date` and `org.joda.time` for date and time handling, which are not thread-safe and lack modern functionality.	It does not have any impact as it is a minor code enhancement. **Workaround:** None	4	25.1.200

Table 4-37 (Cont.) SCP 25.1.200 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
38066384	INVALID_OR_EMPTY_DETAILS errors seen on SCP worker post upgrade of setup to 25.1.200-rc.53 from 25.1.100	INVALID_OR_EMPTY_DETAILS errors are observed on SCP-Worker after upgrading SCP from 25.1.100 to 25.1.200.	Occasional calls from the SCP-Worker pod to get routing rules (custom objects) from notifications have failed. These calls occur every 1 second. Therefore, changes in routing rules might take 1 second more to get realized on SCP-Worker. **Workaround:** None	4	25.1.200
38031000	SCP is selecting the alternate destination on the bases of NF_SET even alternateNFGroupRoutingOptions mode is DNS_SRV and altRoutingDnsSrvModeSupported flag is false	When the `alternateNFGroupRoutingOption` mode is set to `DNS_SRV` and `altRoutingDnsSrvModeSupported` is false, SCP incorrectly selects an alternate route with the same `setID`.	In a specific configuration, SCP performs alternate routing based on `NFSET`, however, it should not happen, as the selected mode of alternate routing is `DNS_SRV` and `altRoutingDnsSrvModeSupported` set to false. **Workaround:** Keep service-based alternate routing as false.	4	25.1.200
38004328	Installation guide has incorrect definition of mediation_status parameter	The `mediation_status` parameter was incorrectly set to true in the `custom.values.yaml` file configuration. This configuration is intended for production use, which may lead to unintended behavior or errors when deployed.	The SCP NF profile that is getting registered with NRF can have the `mediation_status` attribute, which is not required. It has no functional impact. **Workaround:** This attribute can be commented in the SCP deployment file.	4	25.1.100
37627403	Incorrect Message is getting populated when query parameters are given as nf-type="PCF" under NF Rule Profile Data Section	When querying with the `nf-type="PCF"` parameter under the NF Rule Profile Data section, an incorrect error message is displayed, to check the NFTypes-NFServices table, even though PCF nf-type details are available in SCP.	It does not have any functional impact. Only error message correction is required. **Workaround:** None	4	25.1.100
37543889	SubscriptionInfo is getting ignored in case if User comments out customInfo in NRF Details.	If the `customInfo` field is commented out in the NRF profile within the deployment `values.yaml` file and `subscriptionInfo` is set to true with a specified scheme, the code incorrectly ignores the provided scheme and instead extracts the scheme from `ScpInfo`.	This issue appears only if the customInfo section of NrfProfile is removed from the deployment file. **Workaround:** The `subscriptionInfo` parameter is documented in Oracle Communications Cloud Native Core, Service Communication Proxy Installation, Upgrade, and Fault Recovery Guide should not be deleted.	4	25.1.100

Table 4-37 (Cont.) SCP 25.1.200 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36926043	SCP shows unclear match header and body in mediation trigger points	In the Mediation Trigger Points feature, SCP displays unclear text instead of the expected match header and body information.	It does not have any functional impact. **Workaround:** None	4	24.2.0

4.3.10 SEPP Known Bugs

Release 25.1.201

There are no known bugs in this release.

Release 25.1.200

Table 4-38 SEPP 25.1.200 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
37482876	429 error code is being returned despite 428 being configured for rate limiting at SEPP_25.1.0-rc1	The system returns a 429 error code when rate limiting is triggered. The expected behavior is to return error code 428 as defined in the global rate limiting policies. This inconsistency may cause issues in error handling and monitoring processes. Base Bug on Gateway 37497519	Users receive a 429 error code instead of the configured value. This discrepancy prevents any automated actions or responses that rely on the expected error code from being triggered, potentially affecting service reliability and user experience. **Workaround:** There is no workaround available.	3	25.1.100

Table 4-38 (Cont.) SEPP 25.1.200 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
37818065	ERRORs being reported in SEPP plmn egw pod logs intermittently	PLMN Egress Gateway pods intermittently display a "Watcher exception" error, even in the absence of traffic. The error message indicates "too old resource version," with specific values varying, such as "464623931 (554740871)." This issue occurs unexpectedly and may impact the stability of the Egress Gateway pods. Base Bug on Gateway 38082705	The PLMN egress gateway pod generates excessive and unnecessary log entries. **Workaround:** There is no workaround available.	4	25.1.100

Table 4-38 (Cont.) SEPP 25.1.200 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
38015469	SEPP 25.1.100 Custom Values does not expose all containerPortNames	The ocsepp_custom_values_25.1.100.yaml file does not include all the required `containerPortNames` necessary for provisioning `backendPortName` in the CNLB annotations. This omission prevents the correct configuration of backend ports, potentially leading to connectivity issues.	Users are required to manually add parameter and port configurations in the ocsepp_custom_values_25.1.100.yaml file. **Workaround:** Users must manually add the required port in the ocsepp_custom_values_25.1.100.yaml file.	4	25.1.100

Table 4-38 (Cont.) SEPP 25.1.200 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
37969620	Internal server error from SEPP when the payload is bigger than 262144 bytes	An internal server error in SEPP when the payload size exceeds 262,144 bytes and the `Content-Type` is not set to `application/problem+json`. The request gets rejected with a 500 Internal Server Error. The expected behavior is to reject such requests with an HTTP 413 Payload Too Large error, as requests with payloads larger than 262,144 bytes should not be routed through SEPP.	SEPP is able to process messages with size bigger than 262144. The response generated is not in JSON format, and the server header is missing from the response. **Workaround:** There is no workaround available.	3	25.1.100

Table 4-39 SEPP 25.1.200 Gateway Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
35898970	DNS SRV Support- The time taken for cache update is not same TTL value defined in SRV record.	The time taken to update the cache does not align with the Time-To-Live (TTL) value defined in the SRV records. In some cases, the cache updates before the TTL expires, while in others, it updates after the TTL has passed. Expected Behavior The cache should update strictly according to the TTL value specified in the SRV records. For example, if the TTL is set to 60 seconds, the cache must update exactly after every 60-second interval, ensuring consistency with the defined TTL.	When the priority or weight of a record is changed, the cache update may take longer than the defined Time-To-Live (TTL) value. This delay causes the changes to reflect in the environment later than expected. **Workaround:** 1. After modifying the configuration, restart the `n32-egress-gateway` service. 2. Restart the `alternate-route-svc` service to ensure all changes are properly applied.	3	23.4.0

Table 4-39 (Cont.) SEPP 25.1.200 Gateway Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
35919133	DNS SRV Support-Custom values key "dnsSrvEnabled" does not function as decsribed	The description for the custom values key `dnsSrvEnabled` indicates it is a flag to control whether DNS-SRV queries are sent to CoreDNS. If the flag is set to **true**, DNS-SRV queries should be sent to CoreDNS. If the flag is set to **false**, DNS-SRV queries should not be sent to CoreDNS. Issue: Even when the flag is set to **false** and the setup is upgraded, the `curl` request still reaches CoreDNS. Scenario: The flag `dnsSrvEnabled` is set to **false**, and a peer configuration is created for a Virtual Fully Qualified Domain Name (FQDN). The expectation is that running a `curl` command should not resolve the Virtual FQDN because the	For virtual Fully Qualified Domain Names (FQDNs), queries are always directed to CoreDNS, regardless of the configuration settings. **Workaround:** Do not configure records in coreDNS Configuring records in CoreDNS may lead to unintended behavior.	3	23.4.0

Table 4-39 (Cont.) SEPP 25.1.200 Gateway Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
		flag is **false**, and the request should not reach CoreDNS. However, the request is still being sent to CoreDNS, contrary to the expected behavior.			
36263009	PerfInfo calculating ambiguous values for CPU usage when multiple services mapped to single pod	In `cgroup.json` file, multiple services are mapped to a single endpoint. Calculation of CPU usage is ambiguous. This impacted the overall load calculation In the `cgroup.json` file, multiple services are mapped to a single endpoint. This configuration leads to ambiguity in calculating CPU usage for individual services.	The overall load calculation is inaccurate. **Workaround:** There is no workaround available.	3	23.4.1

Table 4-39 (Cont.) SEPP 25.1.200 Gateway Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
36672487	No error thrown while enabling Discard Policy Mapping to true when corresponding discard policy is deleted	No error is thrown when enabling Discard Policy Mapping to **true** for a discard policy that has been deleted. Steps to Reproduce: 1. Delete the discard policy named "Policy2" in the Overload discard policies of the n32 IGW. 2. Enable Discard Policy Mapping to **true** for the policy name "Policy2". The configuration is saved successfully without any error, even though the discard policy "Policy2" has been deleted.	If a user enables discard policy mapping but the corresponding discard policy does not exist, the system does not display an error message. **Workaround:** Users can configure overload discard policies using Helm configuration. This functionality is available and does not cause any known issues.	3	24.2.0

Table 4-39 (Cont.) SEPP 25.1.200 Gateway Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
36605744	Generic error is thrown when wrong configuration is saved via GW REST APIs	A generic error message ("Could not validate JSON") is displayed when an incorrect configuration is saved via the Gateway REST API or CNC Console Screen. The error message does not specify which mandatory parameter is missing or incorrectly configured, making it difficult for users to identify and resolve the issue.	When a generic error occurs, users may find it difficult to identify and troubleshoot the root cause of the issue. **Workaround:** There is no workaround available.	3	24.2.0

Table 4-39 (Cont.) SEPP 25.1.200 Gateway Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found In Release
36614527	[SEPP-APIGW] Overload Control discard policies not working with REST API and CNCC	Users are unable to edit or change the default values for Overload Control discard policies. An error is thrown stating, "ocpolicymapping does not contain this policy name" when attempting to save the configuration. This behavior is observed both when using the CNC Console Screen and when attempting to update the configuration via the REST API.	Users cannot edit overload discard policies through the CNC Console. This limitation restricts the ability to modify these policies directly via the console interface. **Workaround:** Users can configure overload discard policies using Helm configuration.	3	24.2.0

4.3.11 UDR Known Bugs

Release 25.1.200

Table 4-40 UDR 25.1.200 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
38011942	ocudr-custom-values-25.1.100.yaml (used for EIR and SLF) does not expose containerPortNames	The ocudr-custom-values-25.1.100.yaml file used for Equipment Identity Register (EIR) and Subscriber Location Function (SLF) does not expose containerPortNames that are required to provision the backendPortName in the Cloud Native Load Balancer (CNLB) annotations.	There is no impact. **Workaround:** You must change the port names from the internal charts.	3	25.1.100

Table 4-40 (Cont.) UDR 25.1.200 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release

38089584	PROVGW- We observed ERROR log related to alternate-route on PROVGW egress pod	While executing 50K lookups and 1.44K provisioning on the Subscribe Location Function (SLF) site1 through provisioning gateway, an error occurred when scaling the egress gateway from two to zero replicas for 15 minutes and then recovering it back to two replicas. The error is related to the alternate route and was consistently observed on the provgw egress.	There is no impact.
			Workaround:
			You must update the *egressgateway* section of the custom_values yaml file as follows:
			`sbiRouting:`
			`peerConfiguration:`
			`peerSetConfiguration:`
				3	25.1.200

4.3.12 Common Services Known Bugs

4.3.12.1 ATS Known Bugs

Release 25.1.200

There are no known bugs in this release.

4.3.12.2 ASM Configuration Known Bugs

Release 25.1.200

There are no known bugs in this release.

4.3.12.3 Alternate Route Service Known Bugs

Release 25.1.2xx

There are no known bugs in this release.

4.3.12.4 Egress Gateway Known Bugs

Release 25.1.2xx

Table 4-41 Egress Gateway 25.1.2xx Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
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
37886642	Peer configuration and peer set configuration does not work properly in REST mode	The REST API mode revealed issues with the `oc_egressgateway_peer_health_status` metric, where health status updates failed under various peer configuration changes, including dynamic-to-static transitions, FQDN updates, blank configurations, and static-to-dynamic switches. These inconsistencies resulted in incorrect health status data being displayed.	When peer and peerset are configured as blank through the REST mode, oc_egressgateway_peer_health_status of peers do not change. It remains at its previous state. **Workaround**: You must restart the Egress Gateway pods.	3	25.1.200

Table 4-41 (Cont.) Egress Gateway 25.1.2xx Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36730017	Register request towards alternate-route is giving incorrect response of 200	While performing the register request, Gateway Services received a 200 OK response, where the FQDN entry is not present in the DNS server.	While performing Alternate Route Services register request, success response is received when the FQDN entry is absent in the DNS server. **Workaround**: There is no workaround available.	4	24.1.0

4.3.12.5 Ingress Gateway Known Bugs

Release 25.1.2xx

Table 4-42 Ingress Gateway 25.1.2xx Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36464641	When feature Ingress Gateway POD Protection disabled at run time alerts are not getting cleared and metrics are getting pegged in NRF 23.4.0	When the Ingress Gateway Pod Protection feature is disabled at run time, alerts are not getting cleared and metrics are getting pegged in NRF 23.4.0.	Alerts are not getting cleared and metrics would be pegged even when feature is disabled during run time. **Workaround**: There is no workaround available.	3	23.4.0

Table 4-42 (Cont.) Ingress Gateway 25.1.2xx 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 thecontrolledshutdownerrormapping 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**: There is no workaround available.	3	23.2.0
34610831	IGW is accepting incorrect API names with out throwing any error	Ingress Gateway is accepting incorrect API names without displaying any error. If there is a typo in the configuration UDR, the command should get rejected. Otherwise, it gives the wrong impression that the configuration is correct but the desired behavior is not observed.	The non-existing resource name would be pretended to be successfully updated in REST configurations . **Workaround**: There is no workaround available.	3	22.2.4

Table 4-42 (Cont.) Ingress Gateway 25.1.2xx Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36605744	Generic error is thrown when wrong configuration is saved via GW REST APIs	When saving incorrect configurations through the Gateway Services REST API or CNC Console, a generic error, "Could not validate JSON", is displayed instead of providing specific details about the missing mandatory parameters.	A generic error makes it difficult for the user to troubleshoot the issue. **Workaround**: There is no workaround available.	3	24.2.0

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:
			There is no workaround available.
				4	25.1.200

4.3.12.6 Common Configuration Service Known Bugs

Release 25.1.2xx

There are no known bugs in this release.

4.3.12.7 Helm Test Known Bugs

Release 25.1.200

There are no known bugs in this release.

4.3.12.8 Mediation Known Bugs

Release 25.1.200

There are no known bugs in this release.

4.3.12.9 NRF-Client Known Bugs

Release 25.1.2xx

There are no known bugs in this release.

4.3.12.10 App-Info Known Bugs

Release 25.1.2xx

There are no known bugs in this release.

4.3.12.11 Perf-Info Known Bugs

Release 25.1.2xx

There are no known bugs in this release.

4.3.12.12 Debug Tool Known Bugs

Release 25.1.2xx

There are no known bugs in this release.