

Oracle® Communications

Cloud Native Core Release Notes



Release 3.26.1.200.0

G59037-01

August 2026

ORACLE®

Copyright © 2019, 2026, Oracle and/or its affiliates.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software, software documentation, data (as defined in the Federal Acquisition Regulation), or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software," "commercial computer software documentation," or "limited rights data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle®, Java, MySQL, and NetSuite are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Contents

1 Introduction

2 Feature Descriptions

2.1	Automated Testing Suite (ATS) Framework	1
2.2	Cloud Native Environment (CNE)	1
2.3	Operations Services Overlay (OSO)	4
2.4	Cloud Native Core cnDBTier	4
2.5	Cloud Native Configuration Console (CNC Console)	7
2.6	Oracle Communications Cloud Native Core, Certificate Management (OCCM)	8
2.7	Network Repository Function (NRF)	9
2.8	Network Slice Selection Function (NSSF)	11
2.9	OCI Adaptor	12
2.10	Service Communication Proxy (SCP)	12
2.11	Security Edge Protection Proxy (SEPP)	14

3 Media and Documentation

3.1	Media Pack	1
3.2	Impacted Documents	5
3.3	Compatibility Matrix	7
3.4	3GPP Compatibility Matrix	8
3.5	Common Microservices Load Lineup	9
3.6	Generic Open Source Software Compatibility on Any Platform	10
3.7	Redhat Openshift Compliance Matrix	17
3.8	Security Certification Declaration	18
3.8.1	CNC Console Security Certification Declaration	18
3.8.2	cnDBTier Security Certification Declaration	18
3.8.3	OCCM Security Certification Declaration	19
3.8.4	NRF Security Certification Declaration	19
3.8.5	NSSF Security Certification Declaration	20
3.8.6	OCI Adaptor Security Certification	20
3.8.7	SCP Security Certification Declaration	21

4 Resolved and Known Bugs

4.1	Severity Definitions	1
4.2	Resolved Bug List	2
4.2.1	ATS Resolved Bugs	2
4.2.2	cnDBTier Resolved Bugs	2
4.2.3	CNC Console Resolved Bugs	34
4.2.4	CNE Resolved Bugs	36
4.2.5	NSSF Resolved Bugs	37
4.2.6	OSO Resolved Bugs	44
4.2.7	OCCM Resolved Bugs	45
4.2.8	NRF Resolved Bugs	45
4.2.9	SEPP Resolved Bugs	54
4.2.10	SCP Resolved Bugs	60
4.2.11	Common Services Resolved Bugs	71
4.2.11.1	Egress Gateway Resolved Bugs	71
4.2.11.2	Ingress Gateway Resolved Bugs	85
4.2.11.3	Alternate Route Service Resolved Bugs	106
4.2.11.4	Common Configuration Service Resolved Bugs	108
4.2.11.5	NRF-Client Resolved Bugs	109
4.3	Known Bug List	113
4.3.1	ATS Known Bugs	113
4.3.2	CNC Console Known Bugs	113
4.3.3	cnDBTier Known Bugs	114
4.3.4	CNE Known Bugs	117
4.3.5	NSSF Known Bugs	118
4.3.6	OCCM Known Bugs	122
4.3.7	OSO Known Bugs	122
4.3.8	NRF Known Bugs	123
4.3.9	SCP Known Bugs	125
4.3.10	SEPP Known Bugs	136
4.3.11	Common Services Known Bugs	139
4.3.11.1	Alternate Route Service Known Bugs	139
4.3.11.2	Egress Gateway Known Bugs	139
4.3.11.3	Ingress Gateway Known Bugs	141
4.3.11.4	Common Configuration Service Known Bugs	143
4.3.11.5	NRF-Client Known Bugs	143

Preface

- [Documentation Accessibility](#)
- [Diversity and Inclusion](#)

Documentation Accessibility

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

Access to Oracle Support

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

Diversity and Inclusion

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

Conventions

The following text conventions are used in this document:

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

My Oracle Support

My Oracle Support (<https://support.oracle.com>) is your initial point of contact for all product support and training needs.

Use My Oracle Support to access support resources, create and manage Service Requests (SRs), and get assistance with product issues.

For help with My Oracle Support registration, Service Request creation, or other support access questions, use the available support options in My Oracle Support, including MOSFS and MOS Chat.

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

What's New In This Guide

Release 3.26.1.200.0 - G59037-01, August 2026

General Updates

- Updated the open source software compatibility information in the [Generic Open Source Software Compatibility on Any Platform](#) section.
- Updated Redhat Openshift compliance matrix in the [Redhat Openshift Compliance Matrix](#) section.

ATS 26.1.201 Release

Updated the following sections with the details of ATS release 26.1.201:

- [Automated Testing Suite \(ATS\) Framework](#)
- [Media Pack](#)
- [ATS Resolved Bugs](#)

CNC Console 26.1.200 Release

Updated the following sections with the details of CNC Console release 26.1.200:

- [Cloud Native Configuration Console \(CNC Console\)](#)
- [Media Pack](#)
- [Impacted Documents](#)
- [Compatibility Matrix](#)
- [Common Microservices Load Lineup](#)
- [CNC Console Security Certification Declaration](#)
- [CNC Console Resolved Bugs](#)
- [CNC Console Known Bugs](#)

OCCM 26.1.200 Release

Updated the following sections with the details of OCCM release 26.1.200:

- [Oracle Communications Cloud Native Core, Certificate Management \(OCCM\)](#)
- [Media Pack](#)
- [Impacted Documents](#)
- [Compatibility Matrix](#)
- [Common Microservices Load Lineup](#)
- [OCCM Security Certification Declaration](#)

CNE 26.1.200 Release

Updated the following sections with the details of CNE release 26.1.200:

- [Cloud Native Environment \(CNE\)](#)
- [Media Pack](#)
- [Impacted Documents](#)
- [Compatibility Matrix](#)

- [Common Microservices Load Lineup](#)
- [CNE Resolved Bugs](#)
- [CNE Known Bugs](#)

OSO 26.1.200 Release

Updated the following sections with the details of OSO release 26.1.200:

- [Operations Services Overlay \(OSO\)](#)
- [Media Pack](#)
- [Impacted Documents](#)
- [Compatibility Matrix](#)
- [Common Microservices Load Lineup](#)
- [3GPP Compatibility Matrix](#)
- [OSO Resolved Bugs](#)
- [OSO Known Bugs](#)

cnDBTier 26.1.201 Release

Updated the following sections with the details of cnDBTier release 26.1.201:

- [Cloud Native Core cnDBTier](#)
- [Media Pack](#)
- [Impacted Documents](#)
- [Compatibility Matrix](#)
- [Common Microservices Load Lineup](#)
- [3GPP Compatibility Matrix](#)
- [cnDBTier Security Certification Declaration](#)
- [cnDBTier Resolved Bugs](#)
- [cnDBTier Known Bugs](#)

NRF 26.1.201 Release

Updated the following sections with the details of NRF release 26.1.201:

- [Network Repository Function \(NRF\)](#)
- [Media Pack](#)
- [Impacted Documents](#)
- [Compatibility Matrix](#)
- [Common Microservices Load Lineup](#)
- [3GPP Compatibility Matrix](#)
- [NRF Security Certification Declaration](#)
- [NRF Resolved Bugs](#)
- [NRF Known Bugs](#)

NSSF 26.1.201 Release

Updated the following sections with the details of NSSF release 26.1.201:

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

OCI Adaptor 26.1.200 Release

Updated the following sections with the details of OCI Adaptor release 26.1.200:

- [OCI Adaptor](#)
- [Media Pack](#)
- [Compatibility Matrix](#)
- [OCI Adaptor Security Certification](#)

SCP 26.1.201 Release

Updated the following sections with the details of SCP release 26.1.201:

- [Service Communication Proxy \(SCP\)](#)
- [Media Pack](#)
- [Impacted Documents](#)
- [Compatibility Matrix](#)
- [Common Microservices Load Lineup](#)
- [3GPP Compatibility Matrix](#)
- [SCP Security Certification Declaration](#)
- [SCP Resolved Bugs](#)
- [SCP Known Bugs](#)

SEPP 26.1.200 Release

Updated the following sections with the details of SEPP release 26.1.200:

- [Security Edge Protection Proxy \(SEPP\)](#)
- [Media Pack](#)
- [Impacted Documents](#)
- [Compatibility Matrix](#)
- [Common Microservices Load Lineup](#)
- [3GPP Compatibility Matrix](#)
- [SEPP Security Certification Declaration](#)
- [SEPP Resolved Bugs](#)
- [SEPP Known Bugs](#)

Common Services Resolved Bugs

- [Alternate Route Service Resolved Bugs](#)
- [Common Configuration Service Resolved Bugs](#)
- [Egress Gateway Resolved Bugs](#)
- [Ingress Gateway Resolved Bugs](#)
- [NRF-Client Resolved Bugs](#)

Common Services Known Bugs

- [Egress Gateway Known Bugs](#)
- [Ingress Gateway Known Bugs](#)
- [Common Configuration Service 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 3.26.1.2xx.0.

Note

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

2.1 Automated Testing Suite (ATS) Framework

Release 26.1.201

Oracle Communications Cloud Native Core, Automated Test Suite (ATS) Framework 26.1.201 includes the following enhancements:

- **ATS Pod Logs:** ATS pod logs are enhanced with different log categories to provide detailed and structured logging to improve the debugging and analysis process.

Configuration Status: Enabled by default.

For more information about this enhancement, see *Oracle Communications Cloud Native Core Automated Testing Suite Guide*.

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

Table 2-1 License Names for Feature Mapping

License Name	CCNC Number	Feature Name
Enable logging functionality for ATS for debugging purposes	CCNC-12248	ATS Pod Logs

2.2 Cloud Native Environment (CNE)

Release 26.1.200

Oracle Communications Cloud Native Core, Cloud Native Environment (CNE) 26.1.200 has been updated with the following enhancements:

- **Support for Log Externalization:**
CNE supports externalization of logs, allowing users to choose whether to deploy OpenSearch as part of a CNE installation or upgrade. When OpenSearch installation is disabled, Jaeger installation is also disabled.

This feature is useful for deployments that store logging events outside the cluster. Users can optionally install the Fluentd log forwarding mechanism to egress logs from CNE. Currently, only the `http_out` plugin is supported for log egress.

Configuration Status: Disabled by default.

For more information, see the "Log Externalization Support" section in *Oracle Communications Cloud Native Core, Cloud Native Environment User Guide*.

- **Support for VCD 10.6 Platform:**

CNE supports VMware Cloud Director (VCD) 10.6.0 for CNLB VMware deployments. Supported VCD versions are 10.4.3 and 10.6.0.

For more information, see the "Installing vCNE on VMware Environment" section in *Oracle Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide*.

- **Deprecation of LBVM and Transition to Cloud-Native Load Balancers (CNLB):**

CNE supports Cloud-Native Load Balancers (CNLB) only and does not support LBVM-based ingress or egress. Clusters using LBVM with release 25.2.2xx cannot be upgraded to CNE 26.1.200.

The following documents have been updated to remove references to the deprecated LBVM functionality:

- *Oracle Communications Cloud Native Core, Cloud Native Environment User Guide*
- *Oracle Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide*

- **Deprecation of Istio and Cert-manager Components:**

CNE no longer supports Istio or cert-manager. When upgrading from an N-1 or N-2 release to CNE 26.1.200, these components are automatically removed during the upgrade process.

The following documents have been updated to remove references to the deprecated Istio and cert-manager components:

- *Oracle Communications Cloud Native Core, Cloud Native Environment User Guide*
- *Oracle Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide*

- **Support for CNLB Command Line Interface (cnlbctl):**

CNE introduces a command-line utility to support and simplify the management of CNLB-based functionality. The `cnlbctl` command-line interface is available for use from Bastion hosts and can perform several tasks to administer CNLB application management.

Configuration Status: Enabled by default.

For more information, see the "Using CNLB Command Line Utility" section in *Oracle Communications Cloud Native Core, Cloud Native Environment User Guide*.

- **Support for Application Traffic to Bypass CNLB for Ingress and Egress Traffic:**

CNE extends egress bypass support to bare metal platforms. With this feature, users can configure services running on CNE to bypass CNLB when performing egress from the cluster.

Configuration Status: Enabled by default.

For more information, see the "Configuring CNLB Bypass for BareMetal Deployments" 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 - 3.20.0
- Kubernetes - 1.35.2
- podman - 5.6.0
- containerd - 2.2.1
- Calico - 3.30.6
- MetalLB - 0.15.2
- Prometheus - 3.9.0
- OCI-Grafana - 7.5.17
- Jaeger - 2.14.1
- Kyverno - 1.16.1

To get the complete list of third-party services and their versions, refer to the `dependencies_26.1.200.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.

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

Table 2-2 License Names for Feature Mapping

License Name	CCNC Number	Feature Name
Oracle Communications Cloud Native Core, Cloud Native Environment – 25K Active Subscribers Perpetual	CCNC-4765	Log Externalization Support
Oracle Communications Cloud Native Core, Cloud Native Environment – 25K Active Subscribers Perpetual	CCNC-10037	Deprecation of LBVM and Transition to Cloud-Native Load Balancers (CNLB)
Oracle Communications Cloud Native Core, Cloud Native Environment – 25K Active Subscribers Perpetual	CCNC-5201	CNLB Support for FQDN Egress NAT Config
Oracle Communications Cloud Native Core, Advanced Cloud Native Environment – 25K Active Subscribers Perpetual	CCNC-11801	Support for application traffic to Bypass CNLB for Ingress and Egress traffic

Table 2-2 (Cont.) License Names for Feature Mapping

License Name	CCNC Number	Feature Name
Oracle Communications Cloud Native Core, GitOps - Instance Perpetual	CCNC-11034	OC-CNE Integration with GitOps - Support NFs for Integration

2.3 Operations Services Overlay (OSO)

Release 26.1.200

Oracle Communications Cloud Native Core, Operations Services Overlay (OSO) 26.1.200 has been updated with the following enhancements:

- **Secure Kafka Integration for Alert Forwarding:** With this enhancement, the APM microservice now supports TLS-based communication with Kafka. Users can configure the APM service during deployment to establish a secure channel for forwarding alerts to Kafka, thereby improving data security and compliance. APM service also provides the provision of metrics and alerts, which get configured as targets to the OSO Prometheus at the time of installation.

Configuration Status: Enabled by default.

For more information, see the "Alert Forwarding to Kafka" section in *Oracle Communications Cloud Native Core, Operations Services Overlay User Guide*.

- **Support for Leapfrog Upgrade and Rollback:** With this enhancement, OSO supports direct upgrades from up to three prior releases (N+3), reducing the need for sequential upgrades. Leapfrog upgrade support is limited to upgrades targeting 26.1.2xx. Versions earlier than those listed require a sequential upgrade path.

Rollback is also supported for up to three prior releases (N-3) within the defined upgrade and rollback paths.

Configuration Status: This is one time upgrade option, configuration status does not apply.

For more information, see the "Supported Upgrade and Rollback Paths" section in *Oracle Communications Cloud Native Core, Operations Services Overlay Installation and Upgrade Guide*.

- **Deployment Strategy Change:** With this enhancement, the default upgrade behavior for OSO Prometheus pods is updated to use the ReCreate deployment strategy instead of RollingUpdate. This change ensures that existing pods are terminated before new pods are created during an upgrade.

Configuration Status: Set to "ReCreate" by default.

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

2.4 Cloud Native Core cnDBTier

Release 26.1.201

Oracle Communications Cloud Native Core, cnDBTier (cnDBTier) 26.1.201 has been updated with the following enhancements

- **Preferred IP Family and georeplication Stop/Start using CNC Console:**

The CNC Console screens and corresponding cnDBTier APIs have been added to support IP preference selection for the replication channel and to gracefully stop and start georeplication on configured georeplication sites.

This enhancement enables users to perform these operations directly from the CNC Console without requiring manual backend actions.

Note: NF can use the latest menuCncc.json to enable the newly added screens.

Configuration Status: Disabled by default.

For more information, see *Oracle Communications Cloud Native Core, cnDBTier User Guide*

- **Event Details APIs:**

cnDBTier now provides a new set of Event Details APIs hosted on db-monitor-svc to retrieve detailed cnDBTier event information. These APIs return event records that occurred within a caller-specified time window, using startTimestamp and endTimestamp in the request body, and include only events that fall within the defined range.

To control response size and improve retrieval efficiency, the APIs implement pagination, where the caller specifies the number of events per page and the page number through path variables, enabling scalable navigation through large volumes of event data.

Configuration Status: Enabled by default.

For more information, see *Oracle Communications Cloud Native Core, cnDBTier User Guide*

- **Deterministic and Controllable Automatic Georeplication Recovery (GRR):**

cnDBTier now supports deterministic and controllable Automatic Georeplication Recovery (Auto GRR). In earlier releases, Auto GRR always selected the healthy site with the lowest site_id as the backup source and did not allow users to disable automatic recovery during site reinstallation, limiting operational control. With this enhancement, users can enable or disable Auto GRR and specify a preferred backup site for recovery.

New custom_values.yaml parameters:

global.geoReplicationRecovery.autoGRR.enabled: Enables or disables automatic GRR.
Default: true

global.geoReplicationRecovery.preferredBackupSite: Specifies the preferred backup site for GRR.

global.geoReplicationRecovery.backupSiteSelectionPolicy: Defines backup-selection behavior as STRICT or PREFERRED. Default: PREFERRED

New REST APIs are also introduced to GET, UPDATE, and RESET the Auto GRR configuration.

Configuration Status: Enabled by default.

For more information, see *Oracle Communications Cloud Native Core, cnDBTier User Guide*

- **Skip Exception Table Restoration**

cnDBTier now supports skipping data restoration for Exception Tables during the GRR process. A new GRR state, FETCH_RESTORE_EXCLUDED_SCHEMA_DETAILS, has been introduced, in which the failed site calls a REST API on the backup site to retrieve Exception Table details.

The backup site identifies Exception Tables by checking `mysql.ndb_replication` for entries where conflict resolution is enabled and returns the relevant table details. Exception Tables are identified by the \$EX suffix appended to the table name. The failed site stores these details in its Persistent Volume Claim (PVC) and uses the information during restoration to skip data restoration for the Exception Tables.

Only the schema of Exception Tables is restored, not the data. After GRR completes, the Exception Tables exist with their structure intact but remain empty.

Configuration Status: Enabled by default.

For more information, see *Oracle Communications Cloud Native Core, cnDBTier User Guide*

- **CSAR Digital Signature Feature:**

This release introduces digital signing of 5G CNC software packages in CSAR format to meet ETSI NFV-SOL004 V3.5.1 requirements, Section 5.1, Option 1.

The feature applies a cryptographic digital signature to each package to ensure authenticity and integrity during delivery and deployment by verifying that the package has not been altered or corrupted by a third party, whether in transit or at rest. This protects the integrity of 5G network functions throughout the deployment lifecycle.

Configuration Status: Enabled by default.

For more information, see *Oracle Communications Cloud Native Core, cnDBTier User Guide*

- **dbttriage Tool for cnDBTier Health Checks:**

cnDBTier now includes the `dbttriage` tool, which runs a suite of targeted diagnostic tests and provides streaming output along with a final summary report.

The tool performs deeper health checks across cnDBTier sites, including checks for pods and services, replication and georeplication states, and related connectivity and validations. It is intended for DBAs and support engineers to run at one site to quickly validate the health of all database sites and identify common issues, such as pod health problems, replication service failures, or georeplication state inconsistencies.

Configuration Status: Disabled by default.

For more information, see *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*

- **dbtfasterrecover Tool for Replication Recovery:**

cnDBTier now includes the `dbtfasterrecover` tool, which helps restore interrupted bidirectional replication when `db_replication_svc` cannot recover the replication channel automatically.

The tool identifies the latest applied epoch on the local site, selects the next available recovery epoch from the remote site, and configures the local replica to resume replication from the corresponding binary log file and position.

It is intended for DBAs and support engineers to use when replication is broken and a full GRR can potentially be avoided. Post-recovery validation is still required because skipped epochs can result in data inconsistencies between sites.

Configuration Status: Disabled by default.

For more information, see *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*

- **Charset Migration from UTF8MB3 to UTF8MB4:**

The MySQL UTF8MB3 character set is deprecated and will be removed in a future NDB release. Therefore, cnDBTier tables are created with the UTF8MB4 character set starting with this release.

During an upgrade, older tables created using UTF8MB3 are migrated to UTF8MB4 by recreating the tables with UTF8MB4 and repopulating them with the existing records. Because this migration increases the time spent in the pre-upgrade phase, the Helm upgrade must be run with the timeout flag specified in the cnDBTier upgrade guide.

To perform the character set migration successfully, replication must be UP, and there must be no replication lag in any cnDBTier cluster at the time of the upgrade.

For NF, schema definitions must explicitly specify the character set and must never use UTF8. UTF8MB4 is recommended when selecting among UTF8, UTF8MB3, and UTF8MB4.

Configuration Status: Enabled by default.

For more information, see *Oracle Communications Cloud Native Core, cnDBTier User Guide*

- **Password Encryption Enhancement:**

In earlier releases, version 25.2.2xx and earlier, all sites were required to use a common shared password-encryption key. This restriction has now been removed.

Each site can be configured with its own independent and unique password-encryption key, enabling password encryption to be independently enabled or disabled and supporting password rotation at the site level.

This enhancement improves security through key isolation, provides greater flexibility in site-level configurations, and supports GRR when password-encryption keys differ across sites.

Note: The password-encryption feature must be enabled only with cnDBTier 26.1.200 or later. It must not be enabled on earlier cnDBTier versions.

Configuration Status: Disabled by default.

For more information, see *Oracle Communications Cloud Native Core, cnDBTier User Guide*

- **GRR Performance Improvement:**

To improve restoration performance during GRR, this release introduces additional and updated configuration parameters that enhance database-restoration efficiency.

Configuration Status: Enabled by default.

For more information, see *Oracle Communications Cloud Native Core, cnDBTier User Guide*

Note: Network Function license provides cnDBTier capabilities.

2.5 Cloud Native Configuration Console (CNC Console)

Release 26.1.200

Oracle Communications Cloud Native Core, Cloud Native Configuration Console (CNC Console) 26.1.200 includes the following enhancements:

- **CNC Console Support for Open API JSON File:**

CNC Console supports the OpenAPI specification for CNC Console configuration. The `occncc_configuration_openapi_<version>.json` file is delivered as part of the CSAR

package. The `ocncc_configuration_openapi_<version>.json` file contains the OpenAPI specification for CNC Console configuration.

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

- **CNC Console Deployment Using Flux Setup:**

CNC Console supports deployment through a centralized Flux CD setup. The setup uses Helm chart resources to automate deployment to target Kubernetes clusters. Deployment is driven by declarative manifests stored in Git, which helps ensure consistency and version control. This feature was validated with Flux version 2.4.0 and GitLab version v18.2.8-ee for Kubernetes-based environments.

For more information about this enhancement, see the "CNC Console Deployment Using Flux CD Appendix" section *Oracle Communications Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide*.

- **CNC Console IAM Backend Uplift:**

CNC Console includes an IAM backend uplift to address security issues, theme updates, and database schema changes. As part of this uplift, the core procedures for adding or updating passwords, creating and viewing users, configuring SAML IDP, generating access tokens, and managing user federation remained functionally unchanged. The UI screens were refreshed to align with the latest interface and design standards.

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

- **CNCC Database Data Sync Script:**

`dbtdatasync` is a command-line utility that detects, compares, and synchronizes MySQL table data between georeplicated Kubernetes or OpenShift sites. It identifies schema-level and row-level differences, generates compressed dumps and SQL diff files, and supports schema-only validation.

For more information about this enhancement, see the "Database Data Sync Script for CNC Console" section in *Oracle Communications Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide*.

For additional licensing information, see *Oracle Communications Cloud Native Core Licensing Information User Manual*.

Note

Network Function license provides CNC Console capabilities.

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

Release 26.1.200

Oracle Communications Cloud Native Core, Certificate Management (OCCM) 26.1.200 includes the following enhancements:

- **Issuer CA HealthCheck:**

This feature is a lightweight mechanism to regularly monitor the health of OCCM's connectivity with configured issuers (CA) . It does so by configuring a special-purpose certificate termed a HealthCheck Certificate. This certificate is manually created per issuer and configured to renew on configurable interval (preferably daily). This feature enables OCCM to actively verify communication with the Certificate Authority (CA) by initiating certificate lifecycle operations using a dedicated health check certificate. Renewal success or failure events are displayed via a Grafana dashboard, providing real-time visibility into CA integration health. This acts as a proactive monitoring mechanism, helping detect and resolve issues before they impact NF certificates. Instead of performing manual CA health validation, the system:

- Issues a controlled dummy certificate
- Tracks issuance and renewal behavior
- Publishes Prometheus metrics
- Displays real-time status on Grafana dashboard

This enhancement improves system observability without impacting existing certificate workflows. For information, see *Oracle Communications Cloud Native Core, Certificate Management User Guide*.

- **Enhancements using Helm Optimization**

This enhancement optimizes the deployment and upgrade steps for Oracle 5G NFs, reducing the number of steps customers perform in the field to bring up the NFs. For 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 2-3 License Names for Feature Mapping

License Name	CCNC Number	Feature Name
Oracle Communications Cloud Native Core, Certificate Management - 25K Active Subscribers	CCNC-5928	Issuer Health Check
Oracle Communications Cloud Native Core, Certificate Management - 25K Active Subscribers	CCNC-9667	Enhancements via Helm Optimization

2.7 Network Repository Function (NRF)

Release 26.1.201

Oracle Communications Cloud Native Core, Network Repository Function (NRF) 26.1.201 includes the following features or enhancements:

- **Setting SBI Message Priority:** With this feature, support is introduced for setting and forwarding the 3gpp-Sbi-Message-Priority HTTP header as part of the 3GPP SBI Message Priority mechanism. Configuration options are provided to control how the priority header is applied and propagated across NF services.

Configuration Status: Disabled by default.

For more information, see the "Setting SBI Message Priority" section in *Oracle Communications Cloud Native Core, Network Repository Function User Guide*.

- **NF Profile Count Enhancements:** NRF supports a maximum of 1000 NF Profiles in a growth environment configured with two sets. This enhancement improves scalability and capacity for large-scale network deployments.

Configuration Status: Enabled by default.

For more information, see the "NRF Supported Services" section in *Oracle Communications Cloud Native Core, Network Repository Function User Guide*.

- **NF Subscription Limit Enhancements:** With this enhancement, NRF now supports a total of 2000 active NF Subscriptions per segment with Non-Growth and Growth deployment scenarios:
 - **NRF Growth feature disabled:** The entire 2000 active subscription capacity is available within a single set. NRF enforces that the total subscription count within the segment does not exceed this overall limit.
 - **NRF Growth feature enabled:** The total active subscription capacity when in a segment remains 2000, but the subscription allocation is distributed across two sets. The per-set subscription limits are determined by the Growth configuration defined for each set, and NRF ensures that the active subscription count in each set does not exceed its configured limit. Appropriate configuration has to be done to ensure combined subscription limit count in both the NRF sets does not exceed 2000.

Configuration Status: Enabled by default.

For more information, see the "NRF Supported Services" section in *Oracle Communications Cloud Native Core, Network Repository Function User Guide*. For more information about the feature, see the "Subscription Limit" section in *Oracle Communications Cloud Native Core, Network Repository Function User Guide*.

- **Efficient Subscription Notification Processing:** With this enhancement, each subscription microservice pod maintains subscription data in a local in-memory cache instead of retrieving it dynamically from the Cache Data Service (CDS) for every notification event. This improve notification processing efficiency and support higher subscription counts.

Configuration Status: Enabled by default.

For more details, see the "Efficient Subscription Notification Processing" section in *Oracle Communications Cloud Native Core, Network Repository Function User Guide*.

For more details about the feature, contact <https://support.oracle.com>.

- **Gzip Compression for Cache Data Microservice:** This feature adds GZIP compression capabilities in the Cache Data Service (CDS) to reduce payload sizes and optimize bandwidth utilization between NRF microservices such as Discovery, Subscription, and CDS (in CDS-to-CDS communication). It enhances response efficiency for large data transfers by enabling compression at both client and server levels.

Configuration Status: Enabled by default at server side and disabled at client side.

For more details about this feature, see the "GZIP Compression for Cache Data Service" section in *Oracle Communications Cloud Native Core, Network Repository Function User Guide*.

- **Automatic Recovery of Missing NRF Database Records Across Georeplicated Sites:** This feature introduces automatic recovery of missing or inconsistent records in supported database tables across georeplicated NRF sites. Using MySQL NDB replication, a subsequent update can recreate a missing record or synchronize an existing record on peer sites. The feature is enabled by default and requires no separate conflict-resolution mechanism.

Configuration Status: Enabled by default.

For more details, see the "Automatic Recovery of Missing NRF Database Records Across Georeplicated Sites" section in *Oracle Communications Cloud Native Core, Network Repository Function User Guide*.

- **Support for cnDBTier Georeplication Configuration and Control APIs in CNC**

Console: This enhancement introduces APIs to configure IP family preferences and manage georeplication lifecycle (start or stop) across sites in the cnDBTier. It enables users to control replication between site pairs, manage replication groups, and handle switchover readiness through the CNC Console, improving operational control.

Configuration Status: Enabled by default.

For more information, see the "cnDBTier APIs" 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*.

Table 2-4 License Names for Feature Mapping

License Name	License Number	Feature Name
Oracle Communications Cloud Native Core, Network Repository Function - 25K Active Subscribers Perpetual	CCNC-10163	Setting SBI Message Priority
Oracle Communications Cloud Native Core, Network Repository Function - 25K Active Subscribers Perpetual	CCNC-11508	NF Profile Count Enhancements
Oracle Communications Cloud Native Core, Network Repository Function - 25K Active Subscribers Perpetual	CCNC-11510	NF Subscription Limit Enhancements
Oracle Communications Cloud Native Core, Network Repository Function - 25K Active Subscribers Perpetual	CCNC-13829	Efficient Subscription Notification Processing
Oracle Communications Cloud Native Core, Network Repository Function - 25K Active Subscribers Perpetual	CCNC-13827	Gzip Compression for Cache Data Microservice
Oracle Communications Cloud Native Core, Network Repository Function - 25K Active Subscribers Perpetual	CCNC-13825	Automatic Recovery of Missing NRF Database Records Across Georeplicated Sites
Oracle Communications Cloud Native Core, Network Repository Function - 25K Active Subscribers Perpetual	CCNC-12615	Support for cnDBTier Georeplication Configuration and Control APIs in CNC Console

2.8 Network Slice Selection Function (NSSF)

Release 26.1.201

Oracle Communications Cloud Native Core Network Slice Selection Function (NSSF) 26.1.201 has been updated with the following enhancements:

- **Support to Handle Partial NF Profile Update Notifications From NRF:** Enhanced NSSF to support NF_PROFILE_CHANGED notifications with partial updates (profileChanges) in addition to full profiles (nfProfile). This enables faster reaction to peer NSSF state changes (for example, nfStatus) and improves handover decisions in georedundant deployments, while ignoring non-relevant updates and maintaining backward compatibility.

Configuration Status: Disabled by default.

For more information, see the "Support to Handle Partial NF Profile Update Notifications From NRF" 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 2-5 License Names for Feature Mapping

License Name	License Name	Feature Name
Oracle Communications Cloud Native Core, Network Slice Selection Function - 25K Active Subscribers Perpetual	CCNC-6068	Support to Handle Partial NF Profile Update Notifications From NRF

2.9 OCI Adaptor

Release 26.1.200

Oracle Communications Cloud Native Core, OCI Adaptor 26.1.200 has been updated with the following enhancements:

- **Uplifted the OCI Adaptor Components:** The following OCI Adaptor components have been uplifted:
 - Management-agent is uplifted from 1.12.0 to 1.13.0.
 - Fluentd is uplifted from 1.7.4 to 1.7.5.
 - OpenTelemetry Collector image uplifted from 0.124.0 to 0.155.0
- **Uplifted GDK/Micronaut dependency stack:**
 - micronautVersion: 4.10.1-oracle-00001 to 4.10.16-oracle-00001
 - GDK BOM: 4.10.1.4 to 4.10.16
- Removed Metrics Server from OCI Adaptor as it is no longer required and had multiple known vulnerabilities.
- Updated image selection in the Terraform stack user inputs:
 - Removed Node pool Image from OKE Cluster Configuration.
 - Added CLI Server Image under CLI Server Configuration.

2.10 Service Communication Proxy (SCP)

Release 26.1.201

Oracle Communications Cloud Native Core, Service Communication Proxy (SCP) 26.1.201 includes the following enhancements:

- **Next Hop SCP Outlier Detection:** SCP enhances its outlier functionality to detect the next-hop SCP as outlier by determining whether the error response received by consumer SCP-C actually originated from producer SCP-P or not. SCP performs this task by using the oc-3gpp-sbi-od-info header in non-2xx responses generated by SCP-P so SCP-C can determine whether producer SCP-P is healthy or unhealthy.

Configuration Status: Enabled by default (only if the inter SCP Outlier Detection feature is enabled).

For more information, see the "Next Hop SCP Outlier Detection" section in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.

- **Runtime Update for SCP Profile Parameters:** SCP supports modification of certain profile information Helm parameters using REST APIs and the CNC Console during runtime.

Configuration Status: Enabled by default.

For more information, see the "Runtime Update for SCP Profile Parameters" section in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.

- **Support for Subscriber ID to Group ID Resolution:** SCP supports subscriber ID to group ID resolution through the Subscriber Location Function (SLF) lookup functionality of Oracle Communications Cloud Native Core, Unified Data Repository (UDR). SCP performs NF discovery from NRF using the group ID instead of the subscriber ID.

Configuration Status: Disabled by default.

For more information, see the "Support for Subscriber ID to Group ID Resolution" section in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.

- **SCP Capacity Enhancements:** SCP enhances the capabilities of SCPC-Notification and SCPC-Audit microservices to process 3,000 NF profiles.

For more information, see the "SCP Capacity Enhancements" section in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.

- **Verbose Logging for SCP:** SCP has enhanced verbose logging for the SCP-Worker, SCP-nrfProxy, and SCPC-Notification microservices. This feature defines a common log format to include required information to enhance debugging process for WARN and ERROR level logs.

Configuration Status: Enabled by default.

For more information, see the "Verbose Logging for SCP" section in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.

- **TLS Support for SCP to cnDBTier Traffic:** SCP supports secure database connections by using TLS 1.2 or TLS 1.3 and the corresponding cipher suites for the selected TLS version.

Configuration Status: Disabled by default.

For more information, see the "TLS Support for SCP to cnDBTier Traffic" section in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.

- **Rate Limit Enhancements:** SCP enhances its rate limit functionality to support up to 3500 local egress rate limit keys, up to 2400 global egress rate limit keys, and up to 900 ingress rate limit keys.

Configuration Status: Enabled by default.

For more information, see the "Rate Limiting" section in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.

- **SCP Supports Webscale 1.6:** SCP supports Webscale 1.6 with ASM 1.21.

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	License Name	Feature Name
Oracle Communications Cloud Native Core, Service Communication Proxy - 25K Active Subscribers Perpetual	CCNC-5411 and CCNC-12036	Next Hop SCP Outlier Detection
Oracle Communications Cloud Native Core, Service Communication Proxy - 25K Active Subscribers Perpetual	CCNC-9661 and CCNC-12038	Runtime Update for SCP Profile Parameters
Oracle Communications Cloud Native Core, Enhanced Signaling Resiliency - 25K Active Subscribers Perpetual	CCNC-9721 and CCNC-9723	Support for Subscriber ID to Group ID Resolution
Oracle Communications Cloud Native Core, Service Communication Proxy - 25K Active Subscribers Perpetual	CCNC-11551, CCNC-10317, and CCNC-11088	SCP Capacity Enhancements
Oracle Communications Cloud Native Core, Service Communication Proxy - 25K Active Subscribers Perpetual	CCNC-8450 and CCNC-7820	Verbose Logging for SCP
Oracle Communications Cloud Native Core, Service Communication Proxy - 25K Active Subscribers Perpetual	CCNC-5337	TLS Support for SCP to cnDBTier Traffic
Oracle Communications Cloud Native Core, Service Communication Proxy - 25K Active Subscribers Perpetual	CCNC-11549	Rate Limit Enhancements
Oracle Communications Cloud Native Core, Service Communication Proxy - 25K Active Subscribers Perpetual	CCNC-9487	SCP Supports Webscale 1.6

2.11 Security Edge Protection Proxy (SEPP)

Release 26.1.200

Oracle Communications Cloud Native Core, Security Edge Protection Proxy (SEPP) 26.1.200 has been updated with the following enhancements:

- **SEPP Deployment Using Flux Setup:**

SEPP supported deployment through a centralized Flux CD setup. The deployment used Helm chart resources to automate deployment to target Kubernetes clusters. Declarative manifests stored in Git drove the deployment process, which helped maintain consistency and version control. This feature was validated with Flux version 2.4.0 and GitLab version v18.2.8-ee for Kubernetes-based environments.

For more information, see the "SEPP Deployment Using Flux Setup Appendix" section in *Oracle Communications Cloud Native Core, Security Edge Protection Proxy Installation, Upgrade, and Fault Recovery Guide*.

- **SEPP Database Data Sync Script:**

dbtdatasync is a command-line utility that detects, compares, and synchronizes MySQL table data between georeplicated Kubernetes or OpenShift sites. It identifies schema-level and row-level differences, generates compressed dumps and SQL diff files, and supports schema-only validation.

For more information, see the "SEPP Database Data Sync Script Appendix" section in *Oracle Communications Cloud Native Core, Security Edge Protection Proxy Installation, Upgrade, and Fault Recovery Guide*.

- **Support for cnDBTier APIs in CNC Console:**

With this enhancement, the CNC Console GUI displayed the Gracefully Stop Georeplication, Gracefully Start Georeplication, and IP Preference For Replication Channel APIs.

Configuration Status: Enabled by default.

For more information, see the "Support for cnDBTier APIs in CNC Console" section in *Oracle Communications Cloud Native Core, Security Edge Protection Proxy User Guide*.

- **Traffic Segregation Enhancement:**

This enhancement introduced end-to-end traffic segregation for SEPP. It classified and isolated traffic types such as OAM, SBI, and Kubernetes control traffic within a Kubernetes cluster. By using the Multus CNI plugin, SEPP microservice pods could attach to multiple network interfaces. This allowed each traffic type to use a separate network path. Egress traffic from SEPP pods could also be routed through dedicated non-default networks to third-party applications, instead of using a single external network. Cloud-native networking constructs and load balancing mechanisms in OCCNE supported this capability, improving traffic management, scalability, and network reliability.

Configuration Status: Enabled by default.

For more information, see the "Traffic Segregation Enhancement" section in *Oracle Communications Cloud Native Core, Security Edge Protection Proxy User Guide*.

- **Prometheus Alerts Published Directly to Kafka:**

This feature allowed OSO, the Application Processing Microservice, to send alerts outside the cluster as Kafka topics. During testing, the OSO memory profile was increased. The feature was validated by sending 200 alerts per second to OSO through Kafka for 15 minutes.

For more information, see the "SEPP Resource Requirements" section in *Oracle Communications Cloud Native Core, Security Edge Protection Proxy Installation, Upgrade, and Fault Recovery Guide*.

- **SEPP Traffic Prioritization Using Egress Gateway Pod Protection Enhancement:**

Traffic prioritization configuration is now managed through REST-based controls instead of Helm-based configuration. A new CNC Console screen enables configuration of NRF client traffic prioritization, allowing users to define message priorities for all autonomous and on-demand NRF SBI messages.

Configuration Status: Enabled by default.

For more information, see the "SEPP Traffic Prioritization Using Egress Gateway Pod Protection Enhancement" 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 2-7 License Names for Feature Mapping

License Name	License Name	Feature Name
Oracle Communications Cloud Native Core, GitOps	CCNC-9447	SEPP Deployment Using Flux Setup

Table 2-7 (Cont.) License Names for Feature Mapping

License Name	License Name	Feature Name
Oracle Communications Cloud Native Core, Security Edge Protection Proxy - 25K Active Subscribers Perpetual	-	SEPP Database Data Sync Script
Oracle Communications Cloud Native Core, Security Edge Protection Proxy - 25K Active Subscribers Perpetual	-	Support for cnDBTier APIs in CNC Console
Oracle Communications Cloud Native Core, Security Edge Protection Proxy - 25K Active Subscribers Perpetual	CCNC-10383	Traffic Segregation Enhancement
Oracle Communications Cloud Native Core, Security Edge Protection Proxy - 25K Active Subscribers Perpetual	CCNC-11837	Prometheus Alerts Published Directly to Kafka
Oracle Communications Cloud Native Core, Security Edge Protection Proxy - 25K Active Subscribers Perpetual	CCNC-11373	SEPP Traffic Prioritization Using Egress Gateway Pod Protection Enhancement

3

Media and Documentation

3.1 Media Pack

This section lists the media package for Oracle Communications Cloud Native Core 3.26.1.2xx.0. To download the media package, see [MOS](#).

Note

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

Table 3-1 Media Pack Contents for Oracle Communications Cloud Native Core 3.26.1.2xx.0

Description	NF Version	ATS Version	Upgrade Supported
Oracle Communications Cloud Native Configuration Console (CNC Console)	26.1.200	NA	CNC Console 26.1.200 supports fresh installation and upgrade from 25.2.2xx and 25.1.2xx*. For more information, see <i>Oracle Communications Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide</i> . Note: * CNC Console supports upgrade from 25.1.2xx to 26.1.2xx (this exception applies only to upgrade from 25.1.2xx to 26.1.2xx in ASM deployments).
Oracle Communications Cloud Native Core, Certificate Management (OCCM)	26.1.200	NA	OCCM 26.1.200 supports fresh installation and upgrade from 25.2.2xx. For more information, see <i>Oracle Communications Cloud Native Core, Certificate Management Installation and Upgrade Guide</i> . Note: * OCCM supports upgrade from 25.1.2xx to 26.1.2xx (this exception applies only to upgrade from 25.1.2xx to 26.1.2xx in ASM deployments).
Oracle Communications Cloud Native Core, Cloud Native Environment (CNE)	26.1.200	NA	CNE 26.1.200 supports fresh installation and upgrade from 25.2.2xx and 25.2.1xx. For more information, see <i>Oracle Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide</i> .
Oracle Communications Operations Services Overlay (OSO)	26.1.200	NA	OSO 26.1.200 supports fresh installation and upgrade from 25.2.2xx, 25.2.1xx, and 25.1.2xx. For more information, see <i>Oracle Communications Operations Services Cloud Native Core, Overlay Installation and Upgrade Guide</i> .

Table 3-1 (Cont.) Media Pack Contents for Oracle Communications Cloud Native Core 3.26.1.2xx.0

Description	NF Version	ATS Version	Upgrade Supported
Oracle Communications Cloud Native Core, cnDBTier (cnDBTier)	26.1.201	NA	cnDBTier 26.1.201 supports fresh installation and upgrade from 25.2.2xx, 25.2.1xx, and 25.1.2xx. For more information, see <i>Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide</i> .
Oracle Communications Cloud Native Core, Network Repository Function (NRF)	26.1.201	26.1.201	NRF 26.1.201 supports fresh installation and upgrade from 25.2.2xx. For more information, see <i>Oracle Communications Cloud Native Core, Network Repository Function Installation, Upgrade, and Fault Recovery Guide</i> .
Oracle Communications Cloud Native Core, Network Slice Selection Function (NSSF)	26.1.201	26.1.201	NSSF 26.1.201 supports fresh installation and upgrade from 25.2.2xx. For more information, see <i>Oracle Communications Cloud Native Core, Network Slice Selection Function Installation, Upgrade, and Fault Recovery Guide</i> .
Oracle Communications Cloud Native Core, OCI Adaptor	26.1.200	NA	OCI Adaptor 26.1.200 supports fresh installation only. For more information, see <i>Oracle Communications Cloud Native Core, OCI Deployment Guide</i> .
Oracle Communications Cloud Native Core, Service Communications Proxy (SCP)	26.1.201	26.1.201	SCP 26.1.201 supports fresh installation and upgrade from 25.1.2xx and 25.2.2xx. For more information, see <i>Oracle Communications Cloud Native Core, Service Communication Proxy Installation, Upgrade, and Fault Recovery Guide</i> .
Oracle Communications Cloud Native Core, Security Edge Protection Proxy (SEPP)	26.1.200	26.1.200	SEPP 26.1.200 supports fresh installation and upgrade from 25.2.2xx and 25.2.1xx. For more information, see <i>Oracle Communications Cloud Native Core, Security Edge Protection Proxy Installation, Upgrade, and Fault Recovery Guide</i> .

Cloud Native Core Upgrade

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

Figure 3-1 Cloud Native Core Upgrade

Source Releases	Target Releases						
	24.3. x	25.1.1xx	25.1.2xx	25.2.1xx	25.2.2xx	26.1.2xx	26.2.2xx
24.2. x	Y	Y	NS*	NS	NS	NS	NS
24.3. x	NA	Y	Y	NS	NS	NS	NS
25.1.1xx	NA	NA	Y	NS**	NS	NS	NS
25.1.2xx	NA	NA	NA	Y	Y	NS***	NS
25.2.1xx	NA	NA	NA	NA	Y	NS	NS
25.2.2xx	NA	NA	NA	NA	NA	Y	NS
26.1.2xx	NA	NA	NA	NA	NA	NA	Y
26.2.2xx	NA	NA	NA	NA	NA	NA	NA
Legends: NS: Not Supported, NA: Not Applicable, Y: Yes, Upgrade Supported							

Note

- * Policy, CNC Console, UDR, SLF, and cnDBTier support upgrade from 24.2.xx to 25.1.2xx. This exception applies only to upgrade from 24.2.x to 25.1.2xx.
- ** SCP, SEPP, UDR, SLF, CNC Console, and cnDBTier support upgrade from 25.1.1xx to 25.2.1xx. This exception applies only to upgrade from 25.1.1xx to 25.2.1xx.
- *** Policy, CNC Console, and cnDBTier support upgrade from 25.1.2xx to 26.1.2xx. This exception applies only to upgrade from 25.1.2xx to 26.1.2xx in ASM deployments.
- This upgrade guideline is applicable to CNC components except CNE. For CNE upgrade guideline
- This upgrade path is an example and does not show future release plans.
- If the source release is A.B.1xx, upgrades must follow an incremental sequence, for example:
 - A.B.1xx
 - A.B.2xx
 - A.(B+1).1xx
- Skipping intermediate versions, such as A.B.2xx, is not supported.
- Upgrading from A.B.2xx to A.(B+1).2xx is allowed.
- Be sure to select intermediate versions to maintain compatibility throughout the upgrade.

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

CNE Upgrade

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

Figure 3-2 CNE Upgrade

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

Legends: NS: Not Supported, NA: Not Applicable, Y: Yes, Upgrade Supported

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

3.2 Impacted Documents

The following table lists the documents that are impacted in the specific NF release version.

Table 3-2 Impacted Documents

CNC NF	NF Version	Impacted Documents
CNC Console	26.1.200	- Oracle Communications Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide - Oracle Communications Cloud Native Configuration Console User Guide - Oracle Communications Cloud Native Configuration Console Rest Specification Guide - Oracle Communications Cloud Native Configuration Console Troubleshooting Guide - Oracle Communications Cloud Native Configuration Console Network Impact Report
cnDBTier	26.1.201	- Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide - Oracle Communications Cloud Native Core, cnDBTier User Guide - Oracle Communications Cloud Native Core, cnDBTier Network Impact Report - Oracle Communications Cloud Native Core, cnDBTier REST API Guide

Table 3-2 (Cont.) Impacted Documents

CNC NF	NF Version	Impacted Documents
CNE	26.1.200	• Oracle Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide • Oracle Communications Cloud Native Core, Cloud Native Environment User Guide • Oracle Communications Cloud Native Core, Cloud Native Environment Network Impact Report
NSSF	26.1.201	• Oracle Communications Cloud Native Core, Network Slice Selection Function Installation, Upgrade, and Fault Recovery Guide • Oracle Communications Cloud Native Core, Network Slice Selection Function User Guide • Oracle Communications Cloud Native Core, Network Slice Selection Function REST Specification Guide • Oracle Communications Cloud Native Core, Network Slice Selection Function Troubleshooting Guide • Oracle Communications Cloud Native Core, Network Slice Selection Function Network Impact Report
NRF	26.1.201	• Oracle Communications Cloud Native Core, Network Repository Function Installation, Upgrade, and Fault Recovery Guide • Oracle Communications Cloud Native Core, Network Repository Function User Guide • Oracle Communications Cloud Native Core, Network Repository Function Rest Specification Guide • Oracle Communications Cloud Native Core, Network Repository Function Troubleshooting Guide • Oracle Communications Cloud Native Core, Network Repository Function Network Impact Report
OCCM	26.1.200	• Oracle Communications Cloud Native Core, Certificate Management Installation, Upgrade, and Fault Recovery Guide • Oracle Communications Cloud Native Core, Certificate Management User Guide • Oracle Communications Cloud Native Core, Certificate Management REST Specification Guide • Oracle Communications Cloud Native Core, Certificate Management Troubleshooting Guide • Oracle Communications Cloud Native Core, Certificate Management Network Impact Report
OSO	26.1.200	• Oracle Communications Cloud Native Core, Operations Services Overlay Installation and Upgrade Guide • Oracle Communications Cloud Native Core, Operations Services Overlay User Guide • Oracle Communications Cloud Native Core, Operations Services Overlay Network Impact Report
SCP	26.1.201	• Oracle Communications Cloud Native Core, Service Communication Proxy Installation, Upgrade, and Fault Recovery Guide • Oracle Communications Cloud Native Core, Service Communication Proxy User Guide • Oracle Communications Cloud Native Core, Service Communication Proxy REST Specification Guide • Oracle Communications Cloud Native Core, Service Communication Proxy Troubleshooting Guide • Oracle Communications Cloud Native Core, Service Communication Proxy Network Impact Report

Table 3-2 (Cont.) Impacted Documents

CNC NF	NF Version	Impacted Documents
SEPP	26.1.200	• Oracle Communications Cloud Native Core, Security Edge Protection Proxy Installation, Upgrade, and Fault Recovery Guide • Oracle Communications Cloud Native Core, Security Edge Protection Proxy User Guide • Oracle Communications Cloud Native Core Security Edge Protection Proxy Rest Specification Guide • Oracle Communications Cloud Native Core, Security Edge Protection Proxy Troubleshooting Guide • Oracle Communications Cloud Native Core, Security Edge Protection Proxy Network Impact Report

3.3 Compatibility Matrix

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

Note

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

Table 3-3 Compatibility Matrix

CNC NF	NF Version	CNE	cnDBTier	OSO	ASM S/W	Kubernetes	Helm	CNC Console	OCNADD	OCCM	OCI Adaptor
CNC Console	26.1.200	26.1.2xx 25.2.2xx	26.1.2xx 25.2.2xx 25.1.2xx	26.1.2xx 25.2.2xx 25.1.2xx	1.21.6 1.14.6 1.11.8	1.35.x 1.34.x 1.27.x 1.25.x 1.20.x	3.20 3.19.0	NA	26.1.2xx	26.1.2xx	26.1.2xx
OCCM	26.1.200	26.1.2xx 25.2.2xx	NA	NA	NA	1.35.x 1.34.x	3.20 3.19.0	26.1.2xx	NA	NA	NA
CNE	26.1.200	NA	NA	NA	NA	1.35.x	3.20	NA	NA	NA	NA
OSO	26.1.200	NA	NA	NA	NA	1.35.x 1.34.x 1.25.x 1.20.x	3.20 3.19.0	NA	NA	NA	NA

Table 3-3 (Cont.) Compatibility Matrix

CNC NF	NF Version	CNE	cnDBTier	OSO	ASM S/W	Kubernetes	Helm	CNC Console	OCNADD	OCCM	OCI Adaptor
cnDBTier	26.1.201	26.1.2xx 25.2.2xx	NA	26.1.2xx 25.2.2xx 25.1.2xx	1.21.6 1.14.6 1.11.8	1.35.x 1.34.x 1.27.x 1.25.x 1.20.x	3.20 3.19.0	NA	26.1.2x	NA	NA
NRF	26.1.201	26.1.2xx 25.2.2xx	26.1.2xx 25.2.2xx	26.1.2xx 25.2.2xx	1.21.6 1.14.6	1.35.x 1.34.x 1.25.x 1.20.x	3.20 3.19.0	26.1.2xx	26.1.2xx	26.1.2xx	26.1.2xx
NSSF	26.1.201	26.1.2xx 25.2.2xx	26.1.2xx 25.2.2xx	26.1.2xx 25.2.2xx	1.21.6 1.14.6 1.11.8	1.35.x 1.34.x 1.25.x 1.20.x	3.20 3.19.0	26.1.2xx	NA	NA	NA
OCI Adaptor	26.1.200	NA	NA	NA	NA	1.35.x 1.34.x	3.20 3.19.0	NA	NA	NA	NA
SCP	26.1.201	26.1.2xx 25.2.2xx	26.1.2xx 25.2.2xx	26.1.2xx 25.2.2xx	1.21.6 1.14.6 1.11.8	1.35.x 1.34.x 1.27.x 1.25.x 1.20.x	3.20 3.19.0	26.1.2xx	26.1.2xx	26.1.2xx	26.1.2xx
SEPP	26.1.200	26.1.2xx 25.2.2xx	26.1.2xx 25.2.2xx	26.1.2xx 25.2.2xx	1.21.6 1.14.6	1.35.x 1.34.x 1.25.x 1.20.x	3.20 3.19.0	26.1.2xx	26.1.2xx	26.1.2xx	26.1.2xx

3.4 3GPP Compatibility Matrix

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

Table 3-4 3GPP Compatibility Matrix

CNC NF	NF Version	3GPP
CNC Console	26.1.2xx	NA
cnDBTier	26.1.2xx	NA
NSSF	26.1.2xx	3GPP TS 29.531 v15.5.0 3GPP TS 29.531 v16.5.0 3GPP TS 29.531 v16.8.0 3GPP TS 29.501 v16.10.0 3GPP TS 29.502 v16.10.0
OCCM	26.1.2xx	3GPP TS 33.310-h30 3GPP TR 33.876 v0.3.0

Table 3-4 (Cont.) 3GPP Compatibility Matrix

CNC NF	NF Version	3GPP
OSO	26.1.2xx	NA
OCI Adaptor	26.1.2xx	NA
NRF	26.1.2xx	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
SCP	26.1.2xx	3GPP TS 29.504 v18.7 3GPP TS 23.502 v18.7 3GPP TS 29.510 v18.7
SEPP	26.1.2xx	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

Note

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

3.5 Common Microservices Load Lineup

This section provides information about common microservices and ATS for the specific NF versions in Oracle Communications Cloud Native Core Release 3.26.1.2xx.0.

Table 3-5 Common Microservices Load Lineup for Network Functions

CNC NF	NF Version	Alternate Route Svc	App-Info	ASM Configuration	ATS Framework	Config-Server	Debug-tool	Egress Gateway	Ingress Gateway	Helm Test	Mediation	NRF-Client	Perf-Info
CNC Console	26.1.200	NA	NA	NA	NA	NA	26.1.202	NA	26.1.204	26.1.201	NA	NA	NA
OCCM	26.1.200	NA	NA	NA	NA	NA	26.1.202	NA	NA	26.1.201	NA	NA	NA
NSSF	26.1.201	26.1.204	26.1.203	26.1.200	26.1.200	26.1.203	26.1.202	26.1.204	26.1.204	26.1.201	NA	26.1.204	26.1.203
NRF	26.1.201	26.1.205	26.1.203	26.1.200	26.1.201	NA	26.1.202	26.1.205	26.1.205	26.1.201	NA	NA	26.1.203
SCP	26.1.201	NA	NA	26.1.200	26.1.201	NA	26.1.202	NA	NA	26.1.201	26.1.203	NA	NA

Table 3-5 (Cont.) 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	Media tion	NRF-Client	Perf-Info
SEPP	26.1.200	26.1.205	26.1.203	26.1.200	26.1.201	26.1.203	26.1.202	26.1.205	26.1.205	26.1.201	26.1.202	26.1.204	26.1.203

3.6 Generic Open Source Software Compatibility on Any Platform

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

Note

The Software Requirement column in the following table indicates one of the following:

- **Mandatory:** Absolutely essential; the software cannot function without it.
- **Recommended:** Suggested for optimal performance or best practices but not strictly necessary.
- **Conditional:** Required only under specific conditions or configurations.
- **Optional:** Not essential; can be included based on specific use cases or preferences.

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

Software	Tested Software Version		Software Requirement	Category	Sub-Category	Category Requirement	Usage Description
	NF 26.1.2xx	NF 25.2.2xx					
Kubernetes	1.35.2	1.34.1	Mandatory	Orchestration	Container Orchestration	Mandatory	Kubernetes orchestrates scalable, automated NF deployments for high availability and efficient resource utilization. Impact: Preinstallation is required. Without orchestration capabilities, deploying and managing network functions (NFs) can become complex, leading to inefficient resource utilization and potential downtime.

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

Software	Tested Software Version		Software Requirement	Category	Sub-Category	Category Requirement	Usage Description
	NF 26.1.2xx	NF 25.2.2xx					
Helm	3.20.0	3.19.1	Mandatory	Management	Kubernetes Package Management	Mandatory	Helm, a package manager, simplifies deploying and managing NFs on Kubernetes with reusable, versioned charts for easy automation and scaling. Impact: Preinstallation is required. Not using this capability may result in error-prone and time-consuming management of NF versions and configurations, impacting deployment consistency.
Podman	5.6.0	5.6.0	Recommended	Runtime	Containerized NF Image Management	Mandatory	Podman manages and runs containerized NFs without requiring a daemon, offering flexibility and compatibility with Kubernetes. Impact: Preinstallation is required. Podman is a part of Oracle Linux. Without efficient container management, the development and deployment of NFs could become cumbersome, impacting agility.
containerd	2.2.1	2.0.5	Recommended	Runtime	Container Runtime	Mandatory	Containerd manages container lifecycles for running NFs efficiently in Kubernetes. Impact: A lack of a reliable container runtime could lead to performance issues and instability in NF operations.
Velero	1.17.1	1.13.2	Recommended	Backup	Backup and Disaster Recovery for Kubernetes	Optional	Velero backs up and restores Kubernetes clusters for 5G NFs, ensuring data protection and disaster recovery. Impact: Without backup and recovery capabilities, customers would risk data loss and extended downtime, requiring a full cluster reinstall in case of failure or upgrade.

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

Software	Tested Software Version		Software Requirement	Category	Sub-Category	Category Requirement	Usage Description
	NF 26.1.2xx	NF 25.2.2xx					
Kyverno	1.16.1	1.15.0	Recommended	Security	Kubernetes Policy Management	Mandatory	Kyverno is a Kubernetes policy engine that allows to manage and enforce policies for resource configurations within a Kubernetes cluster. Impact: Failing to implement policy enforcement could lead to misconfigurations, resulting in security risks and instability in NF operations, affecting reliability.
MetalLB	0.15.2	0.15.2	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.
CoreDNS	1.12.4	1.12.0	Recommended	Networking	Service Discovery for Kubernetes	Mandatory	CoreDNS is the DNS server in Kubernetes, which provides DNS resolution services within the cluster. Impact: DNS is an essential part of deployment. Without proper service discovery, NFs would struggle to communicate with each other, leading to connectivity issues and operational failures.

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

Software	Tested Software Version		Software Requirement	Category	Sub-Category	Category Requirement	Usage Description
	NF 26.1.2xx	NF 25.2.2xx					
Multus	4.2.2	4.2.1-thick	Recommended	Networking	Networking for Kubernetes traffic segregation	Conditional	Multus enables multiple network interfaces in Kubernetes pods, allowing custom configurations and isolated paths for advanced use cases such as NF deployments, ultimately supporting network segregation. Impact: Without this capability, connecting NFs to multiple networks could be limited, impacting network performance and isolation.
Fluentd	1.19.0	1.17.1	Recommended	Logging	Logging Agent	Mandatory	Fluentd is an open-source data collector that streamlines data collection and consumption, allowing for improved data utilization and comprehension. Impact: Not utilizing centralized logging can hinder the ability to track NF activity and troubleshoot issues effectively, complicating maintenance and support.
OpenSearch	2.19.1	2.18.0	Recommended	Logging	Search/ Analytics/ Logging	Mandatory	OpenSearch provides scalable search and analytics for 5G NFs, enabling efficient data exploration and visualization. Lack of a robust analytics solution could lead to challenges in identifying performance issues and optimizing NF operations, affecting overall service quality.
OpenSearch Dashboard	2.19.1	2.18.0	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 3-6 (Cont.) Generic Open Source Software Compatibility on Any Platform

Software	Tested Software Version		Software Requirement	Category	Sub-Category	Category Requirement	Usage Description
	NF 26.1.2xx	NF 25.2.2xx					
AlertManager	0.30.0	0.28.0	Recommended	Alerting	Alerting (Integration with Prometheus)	Mandatory	Alertmanager is a component that works in conjunction with Prometheus to manage and dispatch alerts. It handles the routing and notification of alerts to various receivers. Impact: Not implementing alerting mechanisms can lead to delayed responses to critical issues, potentially resulting in service outages or degraded performance.
prometheus-kube-state-metric	2.18.0	2.16.0	Recommended	Monitoring	Kubernetes Metrics (for Prometheus)	Mandatory	Kube-state-metrics is a service that generates metrics about the state of various resources in a Kubernetes cluster. It's commonly used for monitoring and alerting purposes. Impact: Without these metrics, monitoring the health and performance of NFs could be challenging, making it harder to proactively address issues.
Prometheus Operator	0.85.0	0.83.0	Recommended	Monitoring	Prometheus Instance Management in Kubernetes	Conditional	The Prometheus Operator is used for managing Prometheus monitoring systems in Kubernetes. Prometheus Operator simplifies the configuration and management of Prometheus instances. Impact: Not using this operator could complicate the setup and management of monitoring solutions, increasing the risk of missed performance insights.
prometheus-node-exporter	1.10.2	1.9.1	Recommended	Monitoring	Node-Level Metrics for Prometheus	Mandatory	Node Exporter is a Prometheus exporter for collecting hardware and OS-level metrics from Linux hosts. Impact: Without node-level metrics, visibility into infrastructure performance would be limited, complicating the identification of resource bottlenecks.

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

Software	Tested Software Version		Software Requirement	Category	Sub-Category	Category Requirement	Usage Description
	NF 26.1.2xx	NF 25.2.2xx					
Prometheus	3.9.0	3.6.0	Mandatory	Monitoring	Metrics/ Monitoring System	Mandatory	Prometheus is a popular open-source monitoring and alerting toolkit. It collects and stores metrics from various sources and allows for alerting and querying. Impact: Not employing this monitoring solution could result in a lack of visibility into NF performance, making it difficult to troubleshoot issues and optimize resource usage.
Grafana	7.5.17	7.5.17	Recommended	Visualization	Monitoring/ Visualization Tool	Mandatory	Grafana is a popular open-source platform for monitoring and observability. It provides a user-friendly interface for creating and viewing dashboards based on various data sources. Impact: Without visualization tools, interpreting complex metrics and gaining insights into NF performance would be cumbersome, hindering effective management.
Calico	3.30.6	3.30.3	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

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

Software	Tested Software Version		Software Requirement	Category	Sub-Category	Category Requirement	Usage Description
	NF 26.1.2xx	NF 25.2.2xx					
metrics-server	0.8.0	0.7.2	Recommended	Monitoring	Resource Metrics for Kubernetes	Mandatory	Metrics server is used in Kubernetes for collecting resource usage data from pods and nodes. Impact: Without resource metrics, auto-scaling and resource optimization would be limited, potentially leading to resource contention or underutilization.
snmp-notifier	2.0.0	2.0.0	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	2.14.1	1.72.0	Recommended	Tracing	Distributed Tracing	Mandatory	Jaeger provides distributed tracing for 5G NFs, enabling performance monitoring and troubleshooting across microservices. Impact: Not utilizing distributed tracing may hinder the ability to diagnose performance bottlenecks, making it challenging to optimize NF interactions and user experience.
rook	1.17.7	1.16.7	Recommended	Storage	Storage Orchestration	Mandatory	Rook is the Ceph orchestrator for Kubernetes that provides storage solutions. It is used in 5G CNE solution. Impact: CSI is mandatory for the solution to work. Not utilizing Rook could increase the complexity of deploying and managing Ceph, making it difficult to scale storage solutions in a Kubernetes environment.

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

Software	Tested Software Version		Software Requirement	Category	Sub-Category	Category Requirement	Usage Description
	NF 26.1.2xx	NF 25.2.2xx					
cinder-csi-plugin	1.35.0	1.33.0	Recommended	Storage	Block Storage Plugin	Mandatory	Cinder CSI (Container Storage Interface) plugin is for provisioning and managing block storage in Kubernetes. It is often used in OpenStack environments to provide persistent storage for containerized applications. Impact: Cinder CSI Plugin is used in OpenStack vCNE solution. Without this integration, provisioning block storage for NFs could be manual and inefficient, complicating storage management.

3.7 Redhat Openshift Compliance Matrix

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

Table 3-7 Redhat Openshift Compliance Matrix

CNC NF Release	Webscale	RH Openshift	K8s	Helm	F5 ASM	F5 SPK
cnDBTier 26.1.2xx	1.3.x	4.7.x	1.20.x	3.19.0	1.11.8	NA
	1.5.x	4.12.x	1.25.x	3.19.0	1.14.6	1.7.11
	1.6.x	4.14.x	1.27.x	3.19.0	1.14.6	1.7.11
OSO 26.1.2xx	1.3.x	4.7.x	1.20.x	3.19.0	1.11.8	NA
	1.5.x	4.12.x	1.25.x	3.19.0	1.14.6	1.7.11
	1.6.x	4.14.x	1.27.x	3.19.0	1.14.6	1.7.11
SCP 26.1.2xx	1.3.x	4.7.x	1.20.x	3.19.0	1.11.8	NA
	1.5.x	4.12.x	1.25.x	3.19.0	1.14.6	1.7.11
	1.6.x	4.14.x	1.27.x	3.19.0	1.14.6	1.7.11
CNCC 26.1.2xx	1.3.x	4.7.x	1.20.x	3.19.0	1.11.8	NA
	1.5.x	4.12.x	1.25.x	3.19.0	1.14.6	1.7.11
	1.6.x	4.14.x	1.27.x	3.19.0	1.14.6	1.7.11
NRF 26.1.2xx	1.3.x	4.7.x	1.20.x	3.19.0	1.11.8	NA
	1.5.x	4.12.x	1.25.x	3.19.0	1.14.6	1.7.11
	1.6.x	4.14.x	1.27.x	3.19.0	1.14.6	1.7.11
NSSF 26.1.2xx	1.3.x	4.7.x	1.20.x	3.19.0	1.11.8	NA
	1.5.x	4.12.x	1.25.x	3.19.0	1.14.6	1.7.11

Table 3-7 (Cont.) Redhat Openshift Compliance Matrix

CNC NF Release	Webscale	RH Openshift	K8s	Helm	F5 ASM	F5 SPK
	1.6.x	4.14.x	1.27.x	3.19.0	1.14.6	1.7.11
SLF 26.1.2xx	1.3.x	4.7.x	1.20.x	3.19.0	1.11.8	NA
	1.5.x	4.12.x	1.25.x	3.19.0	1.14.6	1.7.11
	1.6.x	4.14.x	1.27.x	3.19.0	1.14.6	1.7.11

3.8 Security Certification Declaration

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

3.8.1 CNC Console Security Certification Declaration

Release 26.1.200

Table 3-8 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	July 01, 2026	No unmitigated critical or high findings
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	June 28, 2026	No unmitigated critical or high findings
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	July 01, 2026	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	July 01, 2026	No findings

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

3.8.2 cnDBTier Security Certification Declaration

Release 26.1.201

Table 3-9 cnDBTier Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	July 13, 2026	No unmitigated critical or high findings

Table 3-9 (Cont.) cnDBTier 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	July 13, 2026	No unmitigated critical or high findings
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	July 13, 2026	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	July 13, 2026	No findings

3.8.3 OCCM Security Certification Declaration

Release 26.1.200

Table 3-10 OCCM Security Certification Declaration

Compliance Test Description	Test Completion	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	July 8, 2026	No unmitigated critical or high findings
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	April 8, 2026	No unmitigated critical or high findings
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	July 8, 2026	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	July 8, 2026	No findings

3.8.4 NRF Security Certification Declaration

Release 26.1.201

Table 3-11 NRF Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	July 21, 2026	No unmitigated critical or high findings
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	July 21, 2026	No unmitigated critical or high findings

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

Compliance Test Description	Test Completion Date	Summary
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	July 21, 2026	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	July 21, 2026	No findings

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

3.8.5 NSSF Security Certification Declaration

Release 26.1.201

Table 3-12 NSSF Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Static Source Code Analysis Additional Info: Assesses adherence to common secure coding standards	June 26, 2026	No unmitigated critical or high findings
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	June 26, 2026	No unmitigated critical or high findings
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	June 26, 2026	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	June 26, 2026	No findings

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

3.8.6 OCI Adaptor Security Certification

Release 26.1.200

Table 3-13 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	July 15, 2026	No unmitigated critical or high findings

Table 3-13 (Cont.) OCI Adaptor Security Certification Declaration

Compliance Test Description	Test Completion Date	Summary
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	NA	No unmitigated critical or high findings
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	July 15, 2026	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	July 15, 2026	No findings

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

3.8.7 SCP Security Certification Declaration

Release 26.1.201

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	July 21, 2026	No unmitigated critical or high findings
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	July 21, 2026	No unmitigated critical or high findings
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	July 21, 2026	No unmitigated critical or high finding
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	July 21, 2026	No findings

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

3.8.8 SEPP Security Certification Declaration

Release 26.1.200

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	July 31, 2026	No unmitigated critical or high findings. Scan done through Fortify.
Dynamic Analysis (including fuzz testing) Additional Info: Tests for risk of common attack vectors such as OWASP Top 10 and SANS 25	April 14, 2026	No unmitigated critical, high, medium, and low findings. Scan done through RestFuzz.
Vulnerability Scans Additional Info: Scans for CVEs in embedded 3rd party components	July 31, 2026	No unmitigated critical or high findings. Scan done through Blackduck.
Malware Scans Additional Info: Scans all deliverable software packages for the presence of known malware	July 31, 2026	No issues found. Scan done through McAfee.

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

4

Resolved and Known Bugs

This chapter lists the resolved and known bugs for Oracle Communications Cloud Native Core release 3.26.1.2xx.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 3.26.1.2xx.0.

4.2.1 ATS Resolved Bugs

Release 26.1.201

Table 4-1 ATS 26.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
39176624	ATS UI login fails after scaling up ATS pod due to Jenkins users mismatch when PVC is enabled	ATS GUI login failed after scaling up ATS pod due to Jenkins users mismatch when PVC was enabled (users directory symlink points into jobs). Doc Impact: There is no documentation impact.	2	26.1.200
39004260	ATS API endpoint is not working with IPv6 or Dualstack environment	When ATS was deployed with IPv6 or dualstack deployment mode, ATS API endpoint was unreachable. Doc Impact: There is no documentation impact.	3	26.1.200

Note

Resolved bugs from 25.2.200 have been forward ported to 26.1.201.

4.2.2 cnDBTier Resolved Bugs

Release 26.1.201

Table 4-2 cnDBTier 26.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38982059	Binlog injector thread stall causes epoch not to advance	Binlog injector thread stall caused epoch not to advance. The affected cnDBTier logic and validation were updated to restore the expected behavior. Doc Impact: There is no documentation impact.	2	23.4.6

Table 4-2 (Cont.) cnDBTier 26.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38998915	Replication pod restart could not resolve SSL connection failure on HTTPS-enabled setup	Replication pod restart could not resolve SSL connection failure on HTTPS-enabled setup. Replication and recovery were updated to maintain the expected state and report failures accurately. Doc Impact: There is no documentation impact.	2	25.2.200
39090731	dbtreplmgr reports success without checking replication status	Dbtreplmgr reported success without checking replication status. Replication and recovery handling was updated to maintain the expected state and report failures accurately. Doc Impact: There is no documentation impact.	2	25.2.200
39090743	NDB pods fail to reach ready state when network policy is enabled on OpenShift	NDB pods failed to reach ready state when network policy was enabled on OpenShift. Deployment handling was updated for the affected OpenShift configuration. Doc Impact: There is no documentation impact.	2	25.2.201
39149707	dbtrecover script does not run after phase 0	Dbtrecover script did not run after phase 0. Backup and recovery handling was updated to validate the required state and complete the operation reliably. Doc Impact: There is no documentation impact.	2	25.2.102
39166090	dbtrecovery script does not work with ASM external setup	Dbtrecovery script did not work with ASM external setup. Backup and recovery handling was updated to validate the required state and complete the operation reliably. Doc Impact: There is no documentation impact.	2	25.2.200
39239385	Replication breaks when password encryption key is modified	Replication broke when password encryption key was modified. Replication and recovery handling was updated to maintain the expected state and report failures accurately. Doc Impact: There is no documentation impact.	2	26.1.200

Table 4-2 (Cont.) cnDBTier 26.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
39245979	dbttriage fails at startup because bundled dbtcommon module is missing	Dbttriage failed at startup because bundled dbtcommon module was missing. The affected utility was updated to validate prerequisites, handle startup conditions, and report its result accurately. Doc Impact: There is no documentation impact.	2	26.1.200
39246174	dbtaudit fails because a core Python module is missing	Dbtaudit failed because a core Python module was missing. The affected utility was updated to validate prerequisites, handle startup conditions, and report its result accurately. Doc Impact: There is no documentation impact.	2	26.1.200
39249317	New transporter metrics missing and db-monitor-svc logs continuous errors	New transporter metrics were missing, and db-monitor-svc logged continuous errors. Metrics and monitoring handling was updated so the expected data and behavior were reported correctly. Doc Impact: There is no documentation impact.	2	26.1.200
39257872	Event Details API returns duplicate events and misses unique events across pages	Event Details API returned duplicate events and missed unique events across pages. API processing was updated so it returned consistent results and validated the required state. Doc Impact: There is no documentation impact.	2	26.1.200
39260249	Unsafe scan of ndbinfo.transporters during node restart	An unsafe scan of ndbinfo.transporters occurred during node restart. Pod and node handling was updated to prevent the failure and restore the expected operational state. Doc Impact: There is no documentation impact.	2	24.2.6
39272197	Improve dbtaudit, dbttriage, and dbtfastrecover startup handling for TMPDIR	Startup handling was incomplete for dbtaudit, dbttriage, and dbtfastrecover startup handling for TMPDIR. Backup and recovery handling was updated to validate the required state and complete the operation reliably. Doc Impact: There is no documentation impact.	2	26.1.200

Table 4-2 (Cont.) cnDBTier 26.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
39303878	dbfastrecover reports success despite partial replication	Dbfastrecover reported success despite partial replication. Replication and recovery handling was updated to maintain the expected state and report failures accurately. Doc Impact: There is no documentation impact.	2	26.1.200
39307465	Valid checkpoints are missing in Auto GRR update APIs	Valid checkpoints were missing in Auto GRR update APIs. Replication and recovery handling was updated to maintain the expected state and report failures accurately. Doc Impact: There is no documentation impact.	2	26.1.200
39308966	GRR stuck in RECONFIGURE state	GRR became stuck in RECONFIGURE state. Replication and recovery handling was updated to maintain the expected state and report failures accurately. Doc Impact: There is no documentation impact.	2	26.1.200
39315201	NDB data nodes restart during online backup	NDB data nodes restarted during online backup. Backup and recovery handling was updated to validate the required state and complete the operation reliably. Doc Impact: There is no documentation impact.	2	26.1.200
39318886	Pods fail to pull images from private repository	Pods failed to pull images from private repository. Pod and node handling was updated to prevent the failure and restore the expected operational state. Doc Impact: There is no documentation impact.	2	25.2.201
39324175	Installation fails with a pre-created service account on OpenShift	Installation failed with a pre-created service account on OpenShift. Deployment handling was updated for the affected OpenShift configuration. Doc Impact: There is no documentation impact.	2	26.1.200

Table 4-2 (Cont.) cnDBTier 26.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
39341350	Replication goes down during upgrade because DBTIER_SITE_INFO column conversion fails	Replication went down during upgrade because DBTIER_SITE_INFO column conversion failed. Replication and recovery handling was updated to maintain the expected state and report failures accurately. Doc Impact: There is no documentation impact.	2	26.1.200
39371221	Handle missing GRR metadata tables after failed restore	Handled missing GRR metadata tables after a failed site restore. Updated replication and recovery handling to preserve the expected state and report failures accurately. Doc Impact: There is no documentation impact.	2	26.1.200
39427627	Update site replacement procedure for StatefulSet rollout restart	Updates were required for site replacement procedure for StatefulSet rollout restart. The affected documentation was updated to provide the correct procedure, configuration, or reference information. Doc Impact: Added the rollout restart procedure for all StatefulSets to the site replacement procedure. For more information, see <i>Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide</i> .	2	26.1.200
39445456	SLF 26.1.200 - Observing Ndbmtd pods restarts in multiple containers with different error codes	Configuration options were not exposed fordb_infra_monitor_svc CPU and memory resource settings. The affected cnDBTier logic and validation were updated to restore the expected behavior. Doc Impact: There is no documentation impact.	2	26.1.200

Table 4-2 (Cont.) cnDBTier 26.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
39459517	Document global.imagePullSecrets object-list format for Helm install	Documentation was missing for global.imagePullSecrets object-list format for Helm install. The affected documentation was updated to provide the correct procedure, configuration, or reference information. Doc Impact: Added the global.imagePullSecrets parameter to the "Global Parameters" section. For more information, see <i>Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide</i> .	2	25.2.202
39472791	Prevent LoadBalancer labels on db-replication-svc internal service	The system did not prevent LoadBalancer labels on db-replication-svc internal service. Replication and recovery handling was updated to maintain the expected state and report failures accurately. Doc Impact: There is no documentation impact.	2	26.1.200
39505844	dbtrecover fails on transient replication_info outage during restore	Dbtrecover failed on transient replication_info outage during restore. Replication and recovery handling was updated to maintain the expected state and report failures accurately. Doc Impact: There is no documentation impact.	2	25.2.202
39520233	Fix missing StartNodeId validation before site addition	Incorrect behavior affected missing StartNodeId validation before site addition. Pod and node handling was updated to prevent the failure and restore the expected operational state. Doc Impact: There is no documentation impact.	2	26.1.200

Table 4-2 (Cont.) cnDBTier 26.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
39534327	Update cnDBTier docs for dbtaudit guidance	Updates were required for cnDBTier docs for dbtaudit. The affected documentation was updated to provide the correct procedure, configuration, or reference information. Doc Impact: Updated the section 'Auditing cnDBTier Sites with dbaudit'. For more information, see <i>Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide</i>.	2	25.2.202
39536009	DBTIER_INITIAL_BINLOG_POSITION lacks mate-site entries on fresh deployment	DBTIER_INITIAL_BINLOG_POSITION lacked mate-site entries on a fresh deployment. The affected cnDBTier logic and validation were updated to restore the expected behavior. Doc Impact: There is no documentation impact.	2	26.1.200
39554203	NDB data node hits DBTC assertion during rolling-upgrade failure handling	An NDB data node hit a DBTC assertion during rolling-upgrade failure handling. Pod and node handling was updated to prevent the failure and restore the expected operational state. Doc Impact: There is no documentation impact.	2	26.1.200
39572938	GRR failed on SM Performance Setup because of wrong calculation of Disk sufficiency.	Incorrect behavior affected GRR backup PVC validation using aggregate memory usage. Replication and recovery handling was updated to maintain the expected state and report failures accurately. Doc Impact: There is no documentation impact.	2	26.1.200

Table 4-2 (Cont.) cnDBTier 26.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
39577599	Clarify georeplication credentials and encryption-key guidance	Documentation was unclear about georeplication credentials and encryption-key guidance. The affected documentation was updated to provide the correct procedure, configuration, or reference information. Doc Impact: Updated the password-encryption guidance with credential and encryption-key requirements for georeplication sites. For more information, see <i>Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide</i>.	2	26.1.200
39656682	Document GRR recovery when replication_info is missing after NDB restore failure	Documentation was missing for GRR recovery when replication_info was missing after NDB restore failure. The affected documentation was updated to provide the correct procedure, configuration, or reference information. Doc Impact: Added recovery steps for a missing replication_info database to the "Restoring GR Failures Using cnDBTier GRR APIs" section. For more information, see <i>Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide</i>.	2	26.1.200
39659432	Add grr_info cleanup step to replication recovery guide	Support was missing for grr_info cleanup step to replication recovery guide. Replication and recovery handling was updated to maintain the expected state and report failures accurately. Doc Impact: Added the grr_info cleanup step to the replication recovery procedure. For more information, see <i>Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide</i>.	2	26.1.200

Table 4-2 (Cont.) cnDBTier 26.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
39675735	GRR through dbtrecover fails when Auto GRR is disabled	GRR through dbtrecover failed when Auto GRR was disabled. Replication and recovery handling was updated to maintain the expected state and report failures accurately. Doc Impact: There is no documentation impact.	2	26.1.200
39695536	dbtreplmgr timeout while waiting for expected replication status	dbtreplmgr could time out while waiting for replication to reach the expected status. Replication-status handling was updated to avoid the timeout. Doc Impact: There is no documentation impact.	2	26.1.200
39654370	Replication break after cnDBTier upgrade due to schema-conversion conflict	Replication could break after upgrading cnDBTier from 25.1.201-5 to 26.1.200 because of a schema-conversion conflict. Upgrade and replication handling were updated to prevent the conflict. Doc Impact: There is no documentation impact.	2	26.1.200
39713808	NDB restart during ASM-enabled IPv6 upgrade	During an upgrade from 25.2.201 to 26.1.200 in a three-site NSSF GR IPv6 deployment with ASM enabled, ndbmtd could restart with error 6054 and extend upgrade duration. The upgrade flow was updated to prevent the restart. Doc Impact: There is no documentation impact.	2	26.1.200
39747263	FRR failure indication and credential exposure in execution logs	Fast Replication Recovery (FRR) could fail without a clear recovery-failure indication and could expose MySQL credentials in execution logs. FRR error handling and log sanitization were updated. Doc Impact: There is no documentation impact.	2	26.1.201

Table 4-2 (Cont.) cnDBTier 26.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
39758599	Upgrade and rollback documentation for ASM external-enabled setup	The upgrade and rollback documentation required updates for ASM external-enabled deployments. The documentation was updated to provide the required procedure. Doc Impact: Added the Upgrade and Rollback procedures in the "Migrating cnDBTier to Use ASM for External Communication" section. For more information, see <i>Oracle Communications Cloud Native Core cnDBTier User Guide</i>.	2	26.1.201
39676520	Upgrade failure with large DBTIER_REPL_EVENT_INFO table	An upgrade from 25.2.201 to 26.1.200 could fail when replication_info.DBTIER_REPL_EVENT_INFO contained a large number of entries. Upgrade handling was updated to support this condition. Doc Impact: There is no documentation impact.	2	26.1.201
39561914	GRR backup taken from preferred instead of override site	During GRR, the remote-server backup can be taken from the preferred backup site instead of the configured override site. Doc Impact: Updated the section "cnDBTier Deterministic and Controllable Automatic Georeplication Recovery (GRR)" section to clarify GRR backup-site selection precedence and limitations. For more information, see <i>Oracle Communications Cloud Native Core, cnDBTier User Guide</i>.	2	26.1.200
39553160	dbtaudit failure with password encryption	dbtaudit can fail when password encryption is enabled. Doc Impact: Updated the section "Auditing cnDBTier Sites with dbtaudit" to clarify password-encryption support for dbtaudit. For more information, see <i>Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide</i>.	2	25.2.202

Table 4-2 (Cont.) cnDBTier 26.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38924435	Deleting all CNDB pods across three sites causes unrecoverable replication breakage	Deleting all CNDB pods across three sites caused unrecoverable replication breakage. Replication and recovery handling was updated to maintain the expected state and report failures accurately. Doc Impact: There is no documentation impact.	3	25.2.200
38931127	LoadBalancerClass must be explicitly added for F5 SPK IP assignment	LoadBalancerClass was not added automatically for F5 SPK IP assignment. The affected cnDBTier logic and validation were updated to restore the expected behavior. Doc Impact: There is no documentation impact.	3	25.2.200
38948407	RESTART_SQL_NODES_FOR_BINLOG_THREAD_STALL event observed	A RESTART_SQL_NODES_FOR_BINLOG_THREAD_STALL event was observed. Pod and node handling was updated to prevent the failure and restore the expected operational state. Doc Impact: There is no documentation impact.	3	25.2.200
38958909	Missing Documentation for Immutable External IPs After Replication Setup	Documentation was missing for Immutable External IPs After Replication Setup. The affected documentation was updated to provide the correct procedure, configuration, or reference information. Doc Impact: Added a note stating that external IP addresses were immutable after replication setup to the georeplication configuration procedure. For more information, see <i>Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide</i> .	3	25.2.200
38959055	Replication pod restart occurs while re-establishing georeplication	A replication pod restart occurred while georeplication was being re-established. Replication and recovery handling was updated to maintain the expected state and report failures accurately. Doc Impact: There is no documentation impact.	3	25.2.200

Table 4-2 (Cont.) cnDBTier 26.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38962843	Replication got failed while upgrading the site during new site addition	Replication failed while the site was being upgraded during new site addition. Replication and recovery handling was updated to maintain the expected state and report failures accurately. Doc Impact: There is no documentation impact.	3	25.2.200
38981208	All GRR events are not captured in replication_info.DBTIER_REPL_EVENT_INFO after GRR completion	All GRR events were not captured in replication_info.DBTIER_REPL_EVENT_INFO after GRR completion. Replication and recovery handling was updated to maintain the expected state and report failures accurately. Doc Impact: There is no documentation impact.	3	25.2.200
38983663	Replication goes down after horizontal scaling in a three-site setup	Replication went down after horizontal scaling in a three-site setup. Replication and recovery handling was updated to maintain the expected state and report failures accurately. Doc Impact: There is no documentation impact.	3	25.2.200
39013599	Replication SVC PVC scaling is failing on Non GR/Single site setup	Replication SVC PVC scaling failed on non-GR or single-site setup. Replication and recovery handling was updated to maintain the expected state and report failures accurately. Doc Impact: There is no documentation impact.	3	25.2.200
39026907	Helm test pod logs display No resources found before health-check logs	The Helm test pod displayed "No resources found" before the health-check logs appeared. Pod and node handling was updated to prevent the failure and restore the expected operational state. Doc Impact: There is no documentation impact.	3	25.2.200

Table 4-2 (Cont.) cnDBTier 26.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
39043466	node_type attribute missing in DBTier TC Time Track Metrics	The node_type attribute was missing from DBTier TC Time Track Metrics. Metrics and monitoring handling was updated so the expected data and behavior were reported correctly. Doc Impact: Added the node_type attribute to the DBTier TC Time Track Metrics section. For more information, see <i>Oracle Communications Cloud Native Core, cnDBTier User Guide</i> .	3	25.2.200
39058094	Kyverno policy created during non-ASM deployment is not applied correctly	Kyverno policy created during non-ASM deployment was not applied correctly. The affected cnDBTier logic and validation were updated to restore the expected behavior. Doc Impact: There is no documentation impact.	3	25.2.200
39061324	LOCAL_BACKUP_INITIATE fails when backup_info database does not exist on failed site	LOCAL_BACKUP_INITIATE failed when backup_info database did not exist on failed site. Backup and recovery handling was updated to validate the required state and complete the operation reliably. Doc Impact: There is no documentation impact.	3	25.2.201
39079483	GRR stuck in BACKUPRESTORE state	GRR became stuck in BACKUPRESTORE state. Replication and recovery handling was updated to maintain the expected state and report failures accurately. Doc Impact: There is no documentation impact.	3	25.2.201
39087322	mysql-external-connectivity-service should be removed from custom YAML	Mysql-external-connectivity-service was incorrectly included from custom YAML. The affected cnDBTier logic and validation were updated to restore the expected behavior. Doc Impact: There is no documentation impact.	3	25.2.201
39091105	dbtscale_ndbmt_d_pods must stop on NDB query and sanity failures	Dbtscale_ndbmt_d_pods did not stop on NDB query and sanity failures. Scaling and resource-handling logic was updated to validate values and complete the operation correctly. Doc Impact: There is no documentation impact.	3	25.2.201

Table 4-2 (Cont.) cnDBTier 26.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
39093230	db-replication-svc pods are not prompted for manual restart when automated restart fails during dbtrecover	Db-replication-svc pods were not prompted for manual restart when automated restart failed during dbtrecover. Replication and recovery handling was updated to maintain the expected state and report failures accurately. Doc Impact: There is no documentation impact.	3	25.2.102
39093333	PvcUsageMetricsBuilder fails to read PVC size	PvcUsageMetricsBuilder failed to read PVC size. Metrics and monitoring handling was updated so the expected data and behavior were reported correctly. Doc Impact: There is no documentation impact.	3	25.2.102
39136847	CNCC georeplication status shows down when georeplication is up	CNC Console showed the georeplication status as down when georeplication was up. Replication and recovery handling was updated to maintain the expected state and report failures accurately. Doc Impact: There is no documentation impact.	3	25.2.201
39143347	dbtscale_vertical_pvc updates replication pod PVC values in bytes instead of Gi	Dbtscale_vertical_pvc updated replication pod PVC values in bytes instead of Gi. Replication and recovery handling was updated to maintain the expected state and report failures accurately. Doc Impact: There is no documentation impact.	3	25.2.201
39159515	dbtaudit script does not work in dual-stack deployment	Dbtaudit script did not work in dual-stack deployment. The affected utility was updated to validate prerequisites, handle startup conditions, and report its result accurately. Doc Impact: There is no documentation impact.	3	25.2.100

Table 4-2 (Cont.) cnDBTier 26.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
39221202	Documentation Error: upgradeStrategy and RollingRestart Mentioned Incorrectly	Documentation contained incorrect section references for upgradeStrategy and RollingRestart. The affected documentation was updated to provide the correct procedure, configuration, or reference information. Doc Impact: Corrected the affected section references in the backup and recovery procedures. For more information, see <i>Oracle Communications Cloud Native Core, cnDBTier User Guide</i>	3	26.1.200
39249443	Discrepancy in global.ndb.restoreparallelism documentation value	A discrepancy existed in global.ndb.restoreparallelism documentation value. The affected documentation was updated to provide the correct procedure, configuration, or reference information. Doc Impact: Updated the global.ndb.restoreparallelism parameter in the "Global Parameters" section with the correct value. For more information, see <i>Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide</i> .	3	26.1.200
39254203	Helm chart error while installing cnDBTier 26.1.200	A Helm chart error occurred while cnDBTier 26.1.200 was being installed. The affected cnDBTier logic and validation were updated to restore the expected behavior. Doc Impact: There is no documentation impact.	3	26.1.200
39256558	Prevent empty IPv6 admin_address during ndbappmysqld upgrade startup	The system did not prevent empty IPv6 admin_address during ndbappmysqld upgrade startup. The affected cnDBTier logic and validation were updated to restore the expected behavior. Doc Impact: There is no documentation impact.	3	26.1.200

Table 4-2 (Cont.) cnDBTier 26.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
39270244	cnDBTier Rollback not supported when istiosidecarinject mode:external	The GRR process was not documented for single-site ASM migration. The affected documentation was updated to provide the correct procedure, configuration, or reference information. Doc Impact: Updated the "Migrating cnDBTier to Use ASM for External Communication" section with the GRR steps required for a single-site setup. For more information, see <i>Oracle Communications Cloud Native Core, cnDBTier User Guide</i>.	3	25.2.201
39286747	Pre-upgrade hook completes close to timeout	The pre-upgrade hook completed close to the timeout. The affected cnDBTier logic and validation were updated to restore the expected behavior. Doc Impact: There is no documentation impact.	3	26.1.200
39288509	Alert documentation does not match REPLICATION_DELAY_HIGH implementation	Alert documentation did not match REPLICATION_DELAY_HIGH implementation. The affected documentation was updated to provide the correct procedure, configuration, or reference information. Doc Impact: Updated the REPLICATION_DELAY_HIGH alert description and behavior to match the implemented rule. For more information, see <i>Oracle Communications Cloud Native Core, cnDBTier User Guide</i>.	3	26.1.200
39303366	Horizontal scaling script does not reject incorrect charts	Horizontal scaling script did not reject incorrect charts. Scaling and resource-handling logic was updated to validate values and complete the operation correctly. Doc Impact: There is no documentation impact.	3	26.1.200

Table 4-2 (Cont.) cnDBTier 26.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
39303979	Documentation issue in Event API	Documentation was incorrect in Event API. The affected documentation was updated to provide the correct procedure, configuration, or reference information. Doc Impact: Updated the Event Details API request, response, time-window, and pagination information. For more information, see <i>Oracle Communications Cloud Native Core, cnDBTier REST API Guide</i> .	3	26.1.200
39364230	Add total script execution time output to dbtaudit	dbtaudit did not print total execution time. Backup and recovery handling was updated to validate the required state and complete the operation reliably. Doc Impact: There is no documentation impact.	3	26.1.200
39364277	Add total script execution time output to dbttriage should print total execution time	dbttriage did not print total execution time. Backup and recovery handling was updated to validate the required state and complete the operation reliably. Doc Impact: There is no documentation impact.	3	26.1.200
39365054	Add total script execution time output to dbtfastrecover should print total execution time	Dbtfastrecover did not print total execution time. Backup and recovery handling was updated to validate the required state and complete the operation reliably. Doc Impact: There is no documentation impact.	3	26.1.200
39365473	Improve dbtrecover backup-site messaging	Startup handling was incomplete for dbtrecover backup-site messaging. Backup and recovery handling was updated to validate the required state and complete the operation reliably. Doc Impact: There is no documentation impact.	3	26.1.200

Table 4-2 (Cont.) cnDBTier 26.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
39367733	Missing sample cnDBTier Generic CSAR structure	A sample cnDBTier Generic CSAR structure was missing. The affected documentation was updated to provide the correct procedure, configuration, or reference information. Doc Impact: Added the Generic CSAR directory and file structure to the CSAR package documentation. For more information, see <i>Oracle Communications Cloud Native Core, cnDBTier User Guide</i>.	3	26.1.200
39367847	Duplicate ETSI-Entry-Certificate entry in TOSCA.meta	A duplicate ETSI-Entry-Certificate entry existed in TOSCA.meta. Package validation and deployment content were updated to use the correct files and references. Doc Impact: There is no documentation impact.	3	26.1.200
39372533	Digital validation script does not fail when .sig file is missing	The digital validation script did not fail when the .sig file was missing. Package validation and deployment content were updated to use the correct files and references. Doc Impact: There is no documentation impact.	3	26.1.200
39374079	Fix cs-restricted PSP RoleBinding reference	Incorrect behavior affected cs-restricted PSP RoleBinding reference. Package validation and deployment content were updated to use the correct files and references. Doc Impact: There is no documentation impact.	3	26.1.200
39374255	Definitions/occndbtier.yaml contains incorrect paths in CDCS CSAR	Definitions/occndbtier.yaml contained incorrect paths in CDCS CSAR. Package validation and deployment content were updated to use the correct files and references. Doc Impact: There is no documentation impact.	3	26.1.200

Table 4-2 (Cont.) cnDBTier 26.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
39398750	Pre-upgrade hook fails when stop_repl_switchover contains NULL	Pre-upgrade hook failed when stop_repl_switchover contained NULL. The affected cnDBTier logic and validation were updated to restore the expected behavior. Doc Impact: There is no documentation impact.	3	25.2.102
39417142	Handle empty API_FQDNS in db-monitor datasource selection	Handling was missing for empty API_FQDNS in db-monitor datasource selection. API processing was updated so it returned consistent results and validated the required state. Doc Impact: There is no documentation impact.	3	25.2.201
39418328	Skip heartbeat metrics when replication is not configured	The system did not skip heartbeat metrics when replication was not configured. Metrics and monitoring handling was updated so the expected data and behavior were reported correctly. Doc Impact: There is no documentation impact.	3	25.2.200
39439674	DBTIER_SITE_CONFIG is skipped by dbtremovesite	DBTIER_SITE_CONFIG was skipped by dbtremovesite. The affected cnDBTier logic and validation were updated to restore the expected behavior. Doc Impact: There is no documentation impact.	3	26.1.200
39439891	Add site replacement cleanup for stale DBTIER_REPL_SVC_INFO entries	Support was missing for site replacement cleanup for stale DBTIER_REPL_SVC_INFO entries. The affected cnDBTier logic and validation were updated to restore the expected behavior. Doc Impact: Added the replication_info.DBTIER_REPL_SVC_INFO cleanup step to the site replacement procedure. For more information, see <i>Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide</i> .	3	26.1.200

Table 4-2 (Cont.) cnDBTier 26.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
39460693	DB monitor service throws NullPointerException during initialization	DB monitor service threw NullPointerException during initialization. The affected cnDBTier logic and validation were updated to restore the expected behavior. Doc Impact: There is no documentation impact.	3	26.1.200
39520999	Sync PVC-stored GRR events when parallel recovery is disabled	Synchronization was missing for PVC-stored GRR events when parallel recovery was disabled. Replication and recovery handling was updated to maintain the expected state and report failures accurately. Doc Impact: There is no documentation impact.	3	26.1.200
39521183	Prevent failed or uninstalled sites from being selected as backup	The system did not prevent failed or uninstalled sites from being selected as backup. Backup and recovery handling was updated to validate the required state and complete the operation reliably. Doc Impact: There is no documentation impact.	3	26.1.200
39522690	Add GRR guide note for dummy remoteSiteIp when remote site is failed	Support was missing for GRR guide note for dummy remoteSiteIp when remote site had failed. Replication and recovery handling was updated to maintain the expected state and report failures accurately. Doc Impact: Added a note about using a dummy remoteSiteIp value when the remote site had failed to the GRR procedure. For more information, see <i>Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide</i> .	3	26.1.200

Table 4-2 (Cont.) cnDBTier 26.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
39527608	Document DBTIER_INITIAL_BINLOG_POSTION row-count mismatch behavior	Documentation was missing for DBTIER_INITIAL_BINLOG_POSTION row-count mismatch behavior. The affected documentation was updated to provide the correct procedure, configuration, or reference information. Doc Impact: Added the expected row-count mismatch behavior for DBTIER_INITIAL_BINLOG_POSTION to the dbtaudit troubleshooting information. For more information, see <i>Oracle Communications Cloud Native Core, cnDBTier User Guide</i>.	3	25.2.202
39534838	Update cnDBTier doc for internalService guidance	Updates were required for cnDBTier documents for internalService guidance. The affected documentation was updated to provide the correct procedure, configuration, or reference information. Doc Impact: Added the internalService parameters to the DB Replication Service parameters section. For more information, see <i>Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide</i>.	3	25.2.202
39535060	Clarify dbttriage supported tests in documentation	Documentation was unclear about dbttriage supported tests in documentation. The affected documentation was updated to provide the correct procedure, configuration, or reference information. Doc Impact: Added the supported diagnostic tests to the "Using dbttriage" section. For more information, see <i>Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide</i>.	3	26.1.200

Table 4-2 (Cont.) cnDBTier 26.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
39537317	Fix dbtaudit namespace re-prompting after sourcing source_me	Incorrect behavior affected dbtaudit namespace re-prompting after sourcing source_me. The affected utility was updated to validate prerequisites, handle startup conditions, and report its result accurately. Doc Impact: There is no documentation impact.	3	25.2.202
39543100	Update GRR HTTPS curl examples	Updates were required for GRR HTTPS curl examples. Replication and recovery handling was updated to maintain the expected state and report failures accurately. Doc Impact: Updated the HTTPS curl examples in the "Georeplication Recovery APIs" section to remove --pass and include --cacert. For more information, see <i>Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide</i>.	3	26.1.200
39552371	Fix ndbmysqld scaling procedure when adding a site	Incorrect behavior affected ndbmysqld scaling procedure when adding a site. The affected documentation was updated to provide the correct procedure, configuration, or reference information. Doc Impact: Updated the ndbmysqld pod scaling steps in the "Adding a Georedundant Cluster" procedure. For more information, see <i>Oracle Communications Cloud Native Core, cnDBTier User Guide</i>.	3	26.1.200

Table 4-2 (Cont.) cnDBTier 26.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
39559531	Document source_me prerequisite for dbtfastrecover	Documentation was missing for source_me prerequisite for dbtfastrecover. The affected documentation was updated to provide the correct procedure, configuration, or reference information. Doc Impact: Added the source ./source_me prerequisite to the "Using dbtfastrecover" section. For more information, see <i>Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide</i>.	3	26.1.200
39573289	Correct MYSQL_NDB_CLUSTER_DISCONNECT alert clear behavior documentation	Incorrect behavior affected MYSQL_NDB_CLUSTER_DISCONNECT alert clear behavior documentation. The affected documentation was updated to provide the correct procedure, configuration, or reference information. Doc Impact: Corrected the clear condition for the MYSQL_NDB_CLUSTER_DISCONNECT alert. For more information, see <i>Oracle Communications Cloud Native Core, cnDBTier User Guide</i>.	3	26.1.200
39581697	Clarify dbtrecover backup-site selection policy	Documentation was unclear about dbtrecover backup-site selection policy. The affected documentation was updated to provide the correct procedure, configuration, or reference information. Doc Impact: Added preferred backup site and backup site selection policy behavior to the GRR recovery procedure. For more information, see <i>Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide</i>.	3	26.1.200

Table 4-2 (Cont.) cnDBTier 26.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
39585469	Fix false server_id warnings for sparse multi-site deployments	Incorrect behavior affected false server_id warnings for sparse multi-site deployments. The affected cnDBTier logic and validation were updated to restore the expected behavior. Doc Impact: There is no documentation impact.	3	26.1.200
39587337	Document dbtaudit OpenShift oc namespace handling	Documentation was missing for dbtaudit OpenShift oc namespace handling. The affected documentation was updated to provide the correct procedure, configuration, or reference information. Doc Impact: Added OpenShift oc namespace handling information to the dbtaudit section. For more information, see <i>Oracle Communications Cloud Native Core, cnDBTier User Guide</i>.	3	26.1.200
39587775	Document dbttriage --use-oc namespace requirements	Documentation was missing for dbttriage --use-oc namespace requirements. The affected documentation was updated to provide the correct procedure, configuration, or reference information. Doc Impact: Added the OpenShift namespace requirements for the --use-oc option to the "Using dbttriage" section. For more information, see <i>Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide</i>.	3	26.1.200
39619029	Update GRR state name in Exception Table Restoration documentation	Updates were required for GRR state name in Exception Table Restoration documentation. The affected documentation was updated to provide the correct procedure, configuration, or reference information. Doc Impact: Updated the GRR state name to FETCH_RESTORE_EXCLUDED_SCHEMA_DETAILS in the "Skip Exception Table Restoration" section. For more information, see <i>Oracle Communications Cloud Native Core, cnDBTier User Guide</i>.	3	26.1.200

Table 4-2 (Cont.) cnDBTier 26.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
39658556	Document invalid preferredBackupSite behavior	Documentation was missing for invalid preferredBackupSite behavior. The affected documentation was updated to provide the correct procedure, configuration, or reference information. Doc Impact: Added invalid preferredBackupSite behavior for STRICT and PREFERRED policies to the "Deterministic and Controllable Automatic GRR" section. For more information, see <i>Oracle Communications Cloud Native Core, cnDBTier User Guide</i>.	3	26.1.200
39669973	Add localhost SANs to server certificate	Support was missing for localhost SANs to server certificate. The affected cnDBTier logic and validation were updated to restore the expected behavior. Doc Impact: There is no documentation impact.	3	26.1.200
39675399	Remove obsolete DBTIER_BACKUP_COMM AND_QUEUE cleanup step	Obsolete behavior remained for obsolete DBTIER_BACKUP_COMMAND_QUEUE cleanup step. Backup and recovery handling was updated to validate the required state and complete the operation reliably. Doc Impact: Removed the DBTIER_BACKUP_COMMAND_QUEUE cleanup step from the "Restoring Database From Backup" section. For more information, see <i>Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide</i>.	3	26.1.200

Table 4-2 (Cont.) cnDBTier 26.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
39677883	Documentation issue in site addition procedure	Documentation was incorrect in site addition procedure. The affected documentation was updated to provide the correct procedure, configuration, or reference information. Doc Impact: Corrected the site addition steps in the "Adding a Georedundant Cluster" section. For more information, see <i>Oracle Communications Cloud Native Core, cnDBTier User Guide</i> .	3	26.1.200
39687925	dbtfastrecover fails with AttributeError when db_replication_svc pod is unavailable	Dbtfastrecover failed with AttributeError when db_replication_svc pod was unavailable. Replication and recovery handling was updated to maintain the expected state and report failures accurately. Doc Impact: There is no documentation impact.	3	26.1.200
38915605	Replication service restart during GRR	The db-replication-svc pod can restart with exit code 137 during the GRR procedure. Doc Impact: There is no documentation impact.	3	25.2.200
38585013	dbtscale_vertical_pvc stuck in phase 4	On a non-GR setup, dbtscale_vertical_pvc can remain stuck for an ndbapp pod in phase 4 while waiting for localhost to restart. Doc Impact: There is no documentation impact.	3	25.2.100
38468810	MOP correction for replica start and stop through REST API	The cnDBTier 25.1.200 FR MOP requires correction for starting and stopping a replica through REST APIs. Doc Impact: There is no documentation impact.	3	25.1.200
38884040	PVC values updated in bytes instead of Gi	The dbtscale_vertical_pvc script can update new PVC values in bytes rather than Gi units. Doc Impact: There is no documentation impact.	3	25.1.201
38921972	Replication delay during CNCC upgrade	A replication delay of up to 10 hours (36000 seconds behind remote) can occur during CNCC upgrade. Doc Impact: There is no documentation impact.	3	25.1.200

Table 4-2 (Cont.) cnDBTier 26.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38916012	Cluster disconnect during ndbappmysqlld horizontal scaling	A cluster disconnect can occur when ndbappmysqlld pods are horizontally scaled during DB upgrade from 25.2.100 to 25.2.101. Doc Impact: There is no documentation impact.	3	25.2.200
38877149	Replication break after pod scale-down with skip error enabled	Replication can break when skip error is enabled after ndbmysqlld and ndbappmysqlld pods are completely scaled down for 15 minutes. Doc Impact: There is no documentation impact.	3	25.2.200
39570772	dbtscale_ndbmt_d_pods phase 1 does not exit	Phase 1 of dbtscale_ndbmt_d_pods does not exit when existing NDB data nodes are disconnected or still starting. Doc Impact: There is no documentation impact.	3	25.2.202
39476632	Incorrect backup source selected by dbtrecover	While recovering Site 3, dbtrecover can select Site 4 as the backup source instead of Site 1. Doc Impact: There is no documentation impact.	3	25.2.202
39376809	dbtuser does not work	dbtuser does not work in cnDBTier 25.1.201-4. Doc Impact: There is no documentation impact.	3	25.1.201
39723714	Incorrect GRR GET Config Values API response	The GRR GET Config Values API returns an incorrect response message. Doc Impact: Updated the GET /db-tier/site/{siteName}/config/{configNames} API to correct the response message and remove the stale on-demand backup text. For more information, see <i>Oracle Communications Cloud Native Core, cnDBTier REST API Guide</i> .	3	26.1.200

Table 4-2 (Cont.) cnDBTier 26.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
39735312	replication_skiperror_count does not reset consistently	The replication_skiperror_count column in replication_info.DBTIER_REPL_ERROR_SKIP_INFO does not consistently reset to zero after the expected default 3600-second window. Doc Impact: Updated the section "Using dbtfastrecover" with skip-error limits, reset-window behavior, and recovery actions after a safety limit is exceeded. For more information, see <i>Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide</i>.	3	26.1.200
39278880	False MYSQL_NDB_CLUSTER_DISCONNECT alert on Site 3	A MYSQL_NDB_CLUSTER_DISCONNECT alert can be observed for Site 3 even when the setup is stable. Doc Impact: There is no documentation impact.	3	25.1.103
38948216	Incorrect log message: "Restarting odd pods" but even pod ordinals are listed	The log message incorrectly stated "Restarting odd pods" when even pod ordinals were listed. Pod and node handling was updated to prevent the failure and restore the expected operational state. Doc Impact: There is no documentation impact.	4	25.2.200
38952168	Log displays empty timeout value when waiting for pod	The log displayed an empty timeout value while waiting for a pod. Pod and node handling was updated to prevent the failure and restore the expected operational state. Doc Impact: There is no documentation impact.	4	25.2.200

Table 4-2 (Cont.) cnDBTier 26.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
39074819	Add ASM-only external migration note for istio-inject annotation	Support was missing for ASM-only external migration note for istio-inject annotation. The affected cnDBTier logic and validation were updated to restore the expected behavior. Doc Impact: Added the istio-inject: false requirement to the "Migrating cnDBTier to Use ASM for External Communication" section. For more information, see <i>Oracle Communications Cloud Native Core, cnDBTier User Guide</i> .	4	25.2.201
39202574	Validate backup encryption password and report unsupported characters	Validation was missing for backup encryption password and report unsupported characters. Backup and recovery handling was updated to validate the required state and complete the operation reliably. Doc Impact: There is no documentation impact.	4	25.2.102
39239616	Incorrect Service Reference in LoadBalancerClass Description for sqlgeorepsvclabels	Documentation contained incorrect section references for LoadBalancerClass Description for sqlgeorepsvclabels. The affected documentation was updated to provide the correct procedure, configuration, or reference information. Doc Impact: Corrected the affected section references in the backup and recovery procedures. For more information, see <i>Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide</i> .	4	26.1.200

Table 4-2 (Cont.) cnDBTier 26.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
39239771	Incorrect documentation section references for backup encryption, remote transfer, TDE, and upgrade	Documentation contained incorrect section references for backup encryption, remote transfer, TDE, and upgrade. The affected documentation was updated to provide the correct procedure, configuration, or reference information. Doc Impact: Corrected the affected section references in the backup and recovery procedures. For more information, see <i>Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide</i>.	4	26.1.200
39303483	Update dbtfastrecover documentation for OpenShift execution	Updates were required for dbtfastrecover documentation for OpenShift execution. The affected documentation was updated to provide the correct procedure, configuration, or reference information. Doc Impact: Added the OpenShift command and namespace requirements to the "Using dbtfastrecover" section. For more information, see <i>Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide</i>.	4	26.1.200
39326958	Unable to configure cnDBTier alert rule files on OSO	cnDBTier alert rule files could not be configured on OSO. Metrics and monitoring handling was updated so the expected data and behavior were reported correctly. Doc Impact: There is no documentation impact.	4	26.1.200

Table 4-2 (Cont.) cnDBTier 26.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
39332167	Explain why port 8080 is used as remotesiteport	Documentation did not explain why port 8080 was used as remotesiteport. The affected documentation was updated to provide the correct procedure, configuration, or reference information. Doc Impact: Added an explanation for using port 8080 as remotesiteport to the applicable georeplication procedure. For more information, see <i>Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide</i>.	4	26.1.200
39349551	Mismatch Between Documented and Actual CSAR Test Folder Contents in DB Tier 26.1.200 User Guide	A sample cnDBTier Generic CSAR structure was missing. The affected documentation was updated to provide the correct procedure, configuration, or reference information. Doc Impact: Added the Generic CSAR directory and file structure to the CSAR package documentation. For more information, see <i>Oracle Communications Cloud Native Core, cnDBTier User Guide</i>.	4	26.1.200
39594026	Document expected dbtaudit cross-site inconsistency findings	Documentation was missing for expected dbtaudit cross-site inconsistency findings. The affected documentation was updated to provide the correct procedure, configuration, or reference information. Doc Impact: Added the expected cross-site inconsistency findings to the dbtaudit section. For more information, see <i>Oracle Communications Cloud Native Core, cnDBTier User Guide</i>.	4	26.1.200

Table 4-2 (Cont.) cnDBTier 26.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
39599813	Fix REST API documentation inconsistencies	Incorrect behavior affected REST API documentation inconsistencies. The affected documentation was updated to provide the correct procedure, configuration, or reference information. Doc Impact: Corrected the GeoReplication and Config endpoint paths, parameters, and examples. For more information, see <i>Oracle Communications Cloud Native Core, cnDBTier REST API Guide</i>.	4	26.1.200
39745375	db_tier_client_sql_tps metric not scraped by Prometheus	The db_tier_client_sql_tps metric was generated by ndbappmysqld but was not scraped by Prometheus. Metrics scraping was updated to expose the metric correctly. Doc Impact: There is no documentation impact.	4	25.2.100

Note

Resolved bugs from 25.2.202 have been forward ported to Release 26.1.201.

4.2.3 CNC Console Resolved Bugs

Release 26.1.200

Table 4-3 CNC Console 26.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
39603655	LDAP users were not authenticated after CNCC upgrade to 25.1.202 from 24.2.4	LDAP Test Connection and LDAP login failed in single-stack IPv6 environments because CNCC-IAM/Keycloak was not started with the required IPv6 preference settings. CNCC custom-values support was updated to expose <code>cncc-iam.kc.preferIpv6Stack.enabled</code>, so the required IPv6 JVM preference could be enabled for LDAP connectivity. Upgrade and rollback documentation was also updated to preserve Unicode characters correctly during database backup and restore. Doc Impact: The “Global Configuration Options” section and the upgrade and rollback documentation are updated to include IPv6 preference configuration and Unicode-safe backup and restore guidance in <i>Oracle Communications Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide</i>.	3	25.1.202
39396760	Added tolerationSeconds values for NoExecute toleration in CNCC YAML file	Helm custom-values support was added to configure <code>NoExecute tolerationSeconds</code> for CNCC pods during node not-ready or unreachable conditions. Doc Impact: The “Global Configuration Options” section is updated in <i>Oracle Communications Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide</i>.	3	25.1.200

Table 4-3 (Cont.) CNC Console 26.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
39259142	CNCC Console showed an error while changing the operational state	Operational State Change from the CNCC GUI failed because the request was not sent with the required Content-Type: application/json header. The backend rejected the GUI request even though the same operation worked through REST API. CNCC GUI request handling was corrected so Operational State Change requests were sent with the required Content-Type header. Doc Impact: There is no documentation impact.	3	25.2.101
39387135	Support was required for CNCC ingress configuration in NodePort mode	CNCC did not have code-level support to configure ingress gateway services in NodePort mode. CNCC chart/custom-values handling was updated to support configurable NodePort service type and static HTTP/HTTPS node port configuration for CNCC ingress services such as cncc-iam, mcnc-core, and acnc-core. Doc Impact: The new NodePort custom-values parameters are added in <i>Oracle Communications Cloud Native Configuration Console Installation Guide</i> .	3	25.2.200
39080860	CNCC LDAP server binding credentials via API	CNC Console REST API documentation was updated with additional API endpoints to update LDAP server binding credentials through REST APIs using curl or Postman. Doc Impact: Additional APIs are added in <i>Oracle Communications Cloud Native Configuration Console REST API Guide</i> .	4	24.2.3
39214507	API prefix clarification was required for PCF and BSF API calls through CNCC	The CNC Console User Guide "Accessing NF Configurations Through Curl and Postman" section was updated with examples of Policy and BSF curl requests. Doc Impact: Examples of Policy and BSF curl requests are added in <i>Oracle Communications Cloud Native Configuration Console User Guide</i> .	4	25.2.100

Table 4-3 (Cont.) CNC Console 26.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
39415443	CNCC 25.2.2xx default custom-values parameter had incorrect spelling	The CNC Console parameter <code>global.maxUnavailable</code> contained an incorrect spelling. The parameter was updated in the custom values.yaml file. Doc Impact: The “Global Configuration Options” section is updated in <i>Oracle Communications Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide</i>.	4	25.2.200

Note

Resolved bugs from 25.2.200 have been forward ported to Release 26.1.200.

4.2.4 CNE Resolved Bugs

Release 26.1.200

Table 4-4 CNE 26.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found In Release
39098746	Installation Failure Due to network_optimize.service Start Error	Installation failed when <code>network_optimize.service</code> started on vCNE nodes with a high CPU count because the generated RPS CPU mask value exceeded the supported data type size. The network optimization service, which tunes CNE nodes for optimal and predictable CNLB network performance, caused the installation failure. Doc Impact: There is no documentation impact.	1	26.1.200

Note

Resolved bugs from 25.2.201 have been forward ported to Release 26.1.200.

4.2.5 NSSF Resolved Bugs

Release 26.1.201

Table 4-5 NSSF 26.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
39193463	notifCondition with monitoredAttributes is not present in Subscription request initiated by NSSF in GR.	NSSF did not include notifCondition with monitoredAttributes in subscription requests that it sent to NRF in GR. Doc Impact: There is no documentation impact.	2	26.1.200
39236415	Overload feature is not working because the perf-info service cannot communicate with the Prometheus server getting 503 error response	In 25.2.200, the overload feature did not trigger during 120% and 150% traffic because the perf-info service could not communicate with the Prometheus server and received a 503 response. Doc Impact: There is no documentation impact.	2	25.2.200
39504583	During the L1 Overload scenario, the OSO ALM pod restarted with OOMKilled after the OSO APM pod was intentionally brought down	During an L1 overload scenario in 26.1.200, the OSO ALM pod repeatedly restarted with an OOMKilled condition after the OSO APM pod was intentionally scaled down. Doc Impact: <i>Updated Oracle Communication Cloud Native Core, Operations Services Overlay Installation and Upgrade Guide, section "Configuration of Alert Processing Microservice (APM)" with a limitation that APM supports a single replica deployment and that extended APM unavailability or scale-down to zero replicas can increase Alert Manager memory consumption and cause OOM conditions.</i>	2	26.1.200
39291838	NSSF ATS scenario names contains a typo in the feature file	Several NSSF ATS feature file scenario names contained typographical errors and spelling inconsistencies. Doc Impact: There is no documentation impact.	3	25.2.200
39148715	One of the Availability pods was recreated during the NSSF upgrade, with no changes in the associated Deployment or ConfigMap.	During an upgrade to 26.1.200, one Availability pod was recreated even though the associated Deployment and ConfigMap did not change. Doc Impact: There is no documentation impact.	3	26.1.200

Table 4-5 (Cont.) NSSF 26.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
39582033	CPU allocation for the Leader DB Replication Service need to be increased in custom yaml of CNDB shared with NSSF package	The CPU allocation for the leader DB Replication Service in the CNDB custom YAML shared with the NSSF package needed to be increased from 2 CPUs to 8 CPUs. Doc Impact: There is no documentation impact.	3	26.1.200
39202008	NSSF transitions to Deregistered state instead of Suspended state in NRF when Egress service replicas are scaled to zero	When Egress service replicas were scaled to zero, NSSF moved to the Deregistered state in NRF instead of the Suspended state. Doc Impact: Updated the <i>Oracle Communications Cloud Native Core, Network Slice Selection Function User Guide</i> , "NSSF behaviour when microservices are scaled down" table, to describe NSSF behavior when microservices are scaled down.	3	26.1.200
39322192	NS-Selection 99th percentile latency is higher than IGW for NS-Selection latency in the Grafana dashboard.	During 27K TPS traffic, Grafana showed NS-Selection 99th percentile latency as higher than ingress gateway latency for NS-Selection. Doc Impact: There is no documentation impact.	3	25.2.200
39193092	NSSF 26.1.200: destinationRules should include the hostname in given example in nssf service_mesh custom yaml.	In 26.1.200, the service mesh custom YAML example for CNDB in a different namespace did not work because the destinationRules host did not include the .svc.<cluster_hostname> suffix. Doc Impact: There is no documentation impact.	3	26.1.200
39200060	NSSF should not return a 2xx success response for notifications from NRF containing invalid or non-compliant 3GPP parameters Values.	NSSF returned a 2xx success response for NRF notifications that contained invalid or non-compliant 3GPP parameter values. Doc Impact: Updated the <i>Oracle Communications Cloud Native Core, Network Slice Selection Function User Guide</i> , "Support to Handle Partial NF Profile Update Notifications From NRF" section with in Validation/Error Cases.	3	26.1.200

Table 4-5 (Cont.) NSSF 26.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
39015501	LastUpdateTime field is not getting updated when updating the geo_redundant_sites_info table.	NsSubscription did not update the LastUpdateTime field when it updated the geo_redundant_sites_info table. Doc Impact: There is no documentation impact.	3	25.2.200
39210841	NSSF 26.1.200: Ingress Rate Section in Grafana is not showing any traffic.	In 26.1.200, the Grafana Ingress Rate section showed no traffic, and the related Prometheus query returned no data. Doc Impact: There is no documentation impact.	3	26.1.200
39258489	CNDB pod(ndbappmysqld) restart observed during cnldb upgrade from 25.2.200 to 26.1.200	During a CNDB upgrade from 25.2.200 to 26.1.200, ndbappmysqld pods restarted once on all three CNDB sites, although the upgrade succeeded and no significant traffic drop was observed. Doc Impact: There is no documentation impact.	3	26.1.200
39540527	NSSF Helm charts PDB minAvailable parameter is unused and documentation needs correction	In 25.2.200, the NSSF PodDisruptionBudget Helm charts exposed the unused minAvailable parameter, so the chart values and documentation needed correction to use one active disruption-budget parameter. Doc Impact: There is no documentation impact.	3	25.2.200
39381521	NSSF 25.2.200: alertnative-route replica count mismatch between CIQ and custom values file	In 25.2.200, the Ns-Auditor replica count in the default custom values file did not align with the CIQ, which expected one replica. Doc Impact: There is no documentation impact.	3	25.2.200
39008266	NSSF should reject avail put and patch request if SST type is string.	NSSF accepted an ns-availability PUT request when sst was sent as a string; sst string values in PUT and PATCH requests should have been rejected. Doc Impact: There is no documentation impact.	3	25.2.200

Table 4-5 (Cont.) NSSF 26.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
39031340	With CNDB and NSSF deployed as non-ASM setup in same namespace NSSF installation fails	In 25.2.200 non-ASM mode, NSSF installation failed when CNDB and NSSF were deployed in the same namespace with service mesh disabled because the pre-install hook was denied for a read-only root filesystem policy violation. Doc Impact: There is no documentation impact.	3	25.2.200
38552515	GW Metrics issues for NSSF 54K Success Scenario and 26K failure [Slice is not configured in PlmnInfo] TPS traffic on single site.	In 25.2.200, ingress gateway metrics were incorrect during single-site traffic with 54K successful TPS and 26K failed TPS: 503 responses were not pegged, some 500 responses appeared only in metrics, a 403 invalid-slice reason showed as UNKNOWN, and a backend 403 response was pegged as a 500 response. Doc Impact: There is no documentation impact.	3	25.2.200
38238999	oc_oauth_request_failed_cert_expiry Metric not getting pegged.	The oc_oauth_request_failed_cert_expiry metric was not pegged when a certificate-expired OAuth request returned a 408 response. Doc Impact: There is no documentation impact.	3	25.2.200
35860137	In Policy Mapping Configuration in Ingress Gateway, For the samplingPeriod parameter, max value of parameter validation should be necessary.	In policy mapping configuration, NSSF accepted an excessively large samplingPeriod value and returned a 200 response because maximum value validation was missing. Doc Impact: There is no documentation impact.	3	23.3.0
36552026	KeyId, certName, kSecretName, and certAlgorithm invalid values are not validating in the oauthvalidator configuration.	The OAuth validator configuration accepted invalid keyId, certName, kSecretName, and certAlgorithm values, and validation was also needed in CNCC UI. Doc Impact: There is no documentation impact.	3	24.1.0

Table 4-5 (Cont.) NSSF 26.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
39207188	OAuth error codes not consistent with configuration done in CV file under <code>oauthErrorConfigForValidationFailure</code>	In 26.1.200, OAuth error responses used the correct title and detail but did not use the status codes configured in <code>oauthErrorConfigForValidationFailure</code> for expired-token and KID-mismatch cases. Doc Impact: There is no documentation impact.	3	26.1.200
39503711	duplicate alerts are raised for L1 and L2 Overload Level during performance validation	In 26.1.200, duplicate alerts were raised for L1 and L2 overload levels during performance validation, while previous releases raised one alert for the same condition. Doc Impact: There is no documentation impact.	4	26.1.200
39031454	Removal of deprecated attribute <code>contentEncodingEnabled</code> since this attribute is no longer being used for gzip compression	In 25.2.200, the deprecated <code>contentEncodingEnabled</code> attribute remained in custom YAML even though it was no longer used for gzip compression. Doc Impact: There is no documentation impact.	4	25.2.200
39550656	Continuous Error printing in ns availability pod logs.	The ns-availability pod logs continuously printed Refresh task failed due to invalid response code for k8s api query response. Doc Impact: There is no documentation impact.	4	26.1.200
39200552	The guide shall explicitly document the 3GPP-defined parameter classification for all attributes associated with NRF partial profile update notifications	The guide did not capture the 3GPP classification for NotificationData attributes and Changeltem attributes associated with NRF partial profile update notifications. Doc Impact: Updated the <i>Oracle Communications Cloud Native Core, Network Slice Selection Function User Guide</i> , "Definition of Type NotificationData" and "Definition of Changeltem" tables with condition information for NotificationData and Changeltem.	4	26.1.200
39490095	NSSF 26.1.200: helm success message for NSSF is for installation instead of upgrade	In 26.1.200, Helm upgrade output displayed Thank you for installing ocnsf instead of Thank you for upgrading ocnsf. Doc Impact: There is no documentation impact.	4	26.1.200

Table 4-5 (Cont.) NSSF 26.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
39490028	Clarification Required: NSSF NRF Subscription Deletion Behavior in 3-Site GR Setup (Partial profile)	In a 3-site GR setup, the expected behavior for NSSF NRF subscription deletion was not clearly defined, including the scenarios in which NSSF was expected to delete a subscription. Doc Impact: Updated the <i>Oracle Communications Cloud Native Core, Network Slice Selection Function User Guide</i> , "Support to Handle Partial NF Profile Update Notifications From NRF" section with a note that when NSSF is deregistered from an NRF in a three-site GR deployment, the NRF Client sends a subscription deletion request to the NRF.	4	26.1.200
39231019	Statistics Name Correction Required in Partial Profile Update Notification	The partial profile update notification statistic name did not match between the design page and Prometheus: the design used <code>ocnssf_nrf_invalid_status_notification</code> , and Prometheus used <code>ocnssf_nrf_invalid_status_notification_total</code> . Doc Impact: Updated the <i>Oracle Communications Cloud Native Core, Network Slice Selection Function User Guide</i> , "Support to Handle Partial NF Profile Update Notifications From NRF" and "NSSF Metrics" sections so the metric name is <code>ocnssf_nrf_invalid_status_notification_total</code> .	4	26.1.200
39129294	Removal of enableOutgoingHttps flag under ingress section and incorrect comment added against enableIncomingHttp flag - Duplicate	Bug link description and comments were not accessible; only the issue summary and status were returned. Doc Impact: There is no documentation impact.	4	25.2.200

Table 4-5 (Cont.) NSSF 26.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
39035289	NSSF ATS 25.2.200: ATS Documentation is not same as feature file steps	In 25.2.200, the ATS documentation did not match feature file steps; for example, grsites.feature scenario 02 used a PUT operation with status code 400, while the documentation showed PUT with status code 200. Doc Impact: There is no documentation impact.	4	25.2.200
39031666	Removal of enableOutgoingHttps flag under ingress section and incorrect comment added against enableIncomingHttp flag	In 25.2.200, custom YAML still included the unused enableOutgoingHttps flag under ingress, and the enableIncomingHttp comment incorrectly referred to HTTPS/2.0 instead of HTTP/2.0. Doc Impact: There is no documentation impact.	4	25.2.200
38222239	NSSF Incorrectly Returns "Unsupported Value" Error for Valid SupportedFeature Values (10-15) in ns-availability PUT Request When All Features Are Disabled	When all supported features were disabled, NSSF returned an Unsupported value error for valid SupportedFeature values 10 through 15 in an ns-availability PUT request instead of returning No optional features are supported. Doc Impact: There is no documentation impact.	4	25.2.200
36653494	If KID is missing in access token, NSSF should not send "Kid missing" instead of "kid configured does not match with the one present in the token"	When KID was missing from the access token, NSSF returned the cause kid configured does not match with the one present in the token instead of Kid missing. Doc Impact: There is no documentation impact.	4	24.1.0
39015332	LCI OCI header contains NfInstance ID but does not contain serviceInstanceId	For ns-selection, LCI and OCI headers included NF-Instance but did not include NF-Service-Instance, even though service instance mappings were configured; ns-availability returned both headers. Doc Impact: There is no documentation impact.	4	25.2.200

Table 4-5 (Cont.) NSSF 26.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38941167	Dynamic Logging Feature: With commonCfgClient.enabled set to false run time log level of services is still getting updated	In 25.2.200, runtime log levels for ns-availability and ns-selection were still updated from CNCC even when commonCfgClient.enabled was set to false. Doc Impact: Updated the <i>Oracle Communications Cloud Native Core, Network Slice Selection Function Installation, Upgrade, and Fault Recovery Guide</i> and <i>Oracle Communications Cloud Native Core, Network Slice Selection Function User Guide</i> to state that commonCfgClient.enabled is an engineering parameter with default value true and must not be changed to false.	4	25.2.200

Note

Resolved bugs from 25.1.2xx have been forward ported to Release 26.1.201.

4.2.6 OSO Resolved Bugs

Release 26.1.200

Table 4-6 OSO 26.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
39335185	OSO upgrade failed for RHOC P K8s version 1.20	OSO upgrades on Kubernetes 1.20 clusters failed due to Alertmanager Helm chart compatibility issues. Helm templates are now validated against Kubernetes 1.20, 1.25, and 1.27 to prevent incompatible artifacts from being released. This error was observed because ALM Helm charts were not performing checks on the k8s API for Kubernetes versions 1.20, 1.25, and 1.27. This error has been resolved by adding checks for the k8s version. Doc Impact: There is no documentation impact.	2	26.1.200

Note

Resolved bugs from 25.2.1xx have been forward-ported to Release 26.1.200.

4.2.7 OCCM Resolved Bugs

There are no resolved bugs in this release.

4.2.8 NRF Resolved Bugs

Release 26.1.201

Table 4-7 NRF 26.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
39437130	NRF Auditor pod entered CrashLoopBackOff after a complete connectivity break.	During a complete connectivity break experiment, the NRF Auditor pod restarted repeatedly and entered the CrashLoopBackOff because startup depended on Kubernetes secret access for leader datasource initialization. When secret retrieval failed or timed out, Micronaut treated the bean creation failure as fatal, and the container did not start. This resulted in delayed recovery of the Auditor pod after connectivity was restored. During a fault insertion with a complete connectivity break experiment against the NRF Auditor pod, the auditor pod restarted repeatedly and entered CrashLoopBackOff. The failure was seen during recovery after connectivity interruption, where the pod startup path depended on Kubernetes secret access for leader datasource initialization. The observed customer-facing behavior was that the auditor pod did not recover promptly after connectivity was restored, and recovery could be delayed by Kubernetes restart backoff while startup continued to fail. Doc Impact: There is no documentation impact.	2	26.1.200

Table 4-7 (Cont.) NRF 26.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
39713222	NRF rejected UDR registration requests without Content-Length with a misleading Content-Encoding error.	After NRF was upgraded from 25.1.202 to the 25.2.20x line, previously completed UDR registration requests were rejected when the request body was valid, but the Content-Length header was not specified. NRF returned HTTP 415 with an unsupported Content-Encoding or gzip error even though the failure was related to request transfer framing, not compressed content. This resulted in valid UDR registration requests being rejected with an incorrect error response. Doc Impact: There is no documentation impact.	2	25.2.201
36108386	Forwarding Loop Detection does not consider all the sets of the other NRF segment.	NRF forwarding loop detection did not consider all configured NRF sets in the other segment. When a request contained a Via header from an NRF in a non-primary or lower-priority set, NRF compared the header only with the primary forwarding set and did not detect that the request had already passed through the other segment. This resulted in additional forwarding hops, forwarding loops, and request timeouts in multi-set segment deployments. Doc Impact: Updated the configuration details in the Enhanced NRF Set Based Deployment (NRF Growth) section and updated the recommended actions for the <code>OcnrfSyncFailureFromAllNrfOfAllR</code> <code>emoteSets</code> alert in <i>Oracle Communications Cloud Native Core Network Repository Function User Guide</i>.	3	23.4.0

Table 4-7 (Cont.) NRF 26.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37262850	Server header is not returned in client response by NRF for some error response codes when Support for Server Header feature is enabled.	When the Server header feature was enabled, NRF did not return the configured Server header in some client-facing roaming error responses for the Discovery, Subscription, and Access Token services. NRF propagated the internal Oc-Skip-Server-Header marker for responses generated by the Egress Gateway microservice, and the Ingress Gateway microservice interpreted this marker as an instruction to skip Server header injection. This resulted in client-facing error responses being returned without the configured Server header even though the feature was enabled. Doc Impact: There is no documentation impact.	3	24.3.0
38460687	NRF uses only local site data when georedundancy feature is enabled.	NRF used only local site state data when georedundancy was enabled with overrideReplicationCheck set to true. During a fresh install or georedundancy reconfiguration, updated site mappings from geoRedundancyOptions.siteNameToNrfInstanceldMappingList were not reloaded dynamically, preventing remote site replication status from being updated correctly. This resulted in NRF operating as a standalone site and not considering the configured georedundant site data during service operations until the affected pods were restarted. Doc Impact: Updated the description of global.overrideReplicationCheck in <i>Oracle Communications Cloud Native Core Network Repository Function Installation, Upgrade, and Fault Recovery Guide</i>.	3	25.1.200
39029736	NRF accepted serverHeaderValueBasedSLFSelection as an array instead of a string.	NRF did not reject an invalid array value for serverHeaderValueBasedSLFSelection, even though the configuration field accepted only a string value. This resulted in invalid configuration payloads being accepted instead of being rejected with an appropriate validation error. Doc Impact: There is no documentation impact.	3	25.2.200

Table 4-7 (Cont.) NRF 26.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
39205839	NRF sent nfServices in the notification request instead of nfServiceList during NF Update PUT.	NRF processed a complete NF profile update successfully, but the NF_PROFILE_CHANGED notification could contain nfServices instead of the expected nfServiceList when requesterFeatures=1 requested service-map behavior. The issue also applied to the heartbeat update path when service load changes triggered the same notification flow. This resulted in subscribers receiving a notification payload with the wrong service attribute representation. Doc Impact: There is no documentation impact.	3	25.2.201
39280716	Remote NRF delete subscription request did not persist the unsubscribed state.	In a georedundant NRF deployment, a subscription delete request sent to the remote site returned HTTP 204 even when the remote site did not persist the expected local unsubscribe state. When the record was missing, NRF did not create or update the subscription entry with subscriptionStatus=UNSUBSCRIBED and the remote NRF instance ID as recordOwner. This resulted in the remote site returning success without recording the unsubscribe state required for georedundancy tracking. Doc Impact: There is no documentation impact.	3	25.2.200
39290977	NRF intermittently fell back to DB during performance runs.	During high-throughput NRF performance runs, ocnrf_db_fallback_total increased intermittently because service operations did not consistently use the full cached NRF set data. Under the 53k TPS call model with growth, SLF, forwarding, 1000 NFs, 2000 subscriptions, and ASM enabled, NRF fell back to DB or same-set data paths. This resulted in random DB fallback behavior across service operations under load. Doc Impact: There is no documentation impact.	3	26.1.200

Table 4-7 (Cont.) NRF 26.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
39305975	Subscription based on nfGroupId was treated as duplicate when an nfType subscription already existed and allowDuplicateSubscriptions was false.	When allowDuplicateSubscriptions was set to false, NRF treated a new subscription that included both nfType and nfGroupId as a duplicate of an existing nfType-only subscription. The request returned 201 but reused the first subscription ID instead of creating a distinct group-specific subscription. This resulted in logically different subscriptions being collapsed into the same subscription record. Doc Impact: There is no documentation impact.	3	26.1.200
39374541	NRF hook jobs and AppInfo did not consistently use the configured service account.	NRF hook jobs did not consistently render,serviceAccountName, and AppInfo chart behavior did not reliably use the configured global.serviceAccountName. When image pull secrets were attached only to the configured service account, the affected resources could run with a different identity or fail image pulls in private registry environments. This resulted in inconsistent service account usage for hook jobs and AppInfo-related resources. Doc Impact: There is no documentation impact.	3	26.1.200
39459529	DNS NAPTR records were not cleaned up after AMF NFProfile Update removed amfInfo.n2InterfaceAmfInfo.	After a complete NFProfile Update was removed amfInfo.n2InterfaceAmfInfo, NRF did not remove the previously created DNS NAPTR, A, and AAAA records when DNS NAPTR was enabled. The update succeeded, but stale DNS entries remained in OCDNS. This resulted in DNS records remaining after the AMF N2 information was removed from the NF profile. Doc Impact: There is no documentation impact.	3	26.1.200

Table 4-7 (Cont.) NRF 26.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
39529196	Prometheus showed multiple load levels for performance pods.	Prometheus showed more than one load_level entry for performance services because the queries included stale or non-current leader pod metrics. Filtering only by isLeaderPod="True" did not fully exclude old leader data after leader changes. This resulted in multiple load levels being displayed for the same performance service. Doc Impact: There is no documentation impact.	3	26.1.200
39580529	NRF preferredTaiMatchInd was incorrect for preferred TAI discovery with network and operator DNN portions.	NRF discovery returned preferredTaiMatchInd=false for SMF preferred-TAI discovery when the request used a full DNN with network and operator portions and the registered SMF profile contained only the network identifier DNN. The profiles were still returned, but the preferred-TAI joint match logic did not recognize the equivalent DNN forms. This resulted in an incorrect preferred-TAI match indication during SMF selection. Doc Impact: There is no documentation impact.	3	25.2.201
39659430	Alternate-route service did not define ephemeralStorageLimit, so the ephemeral-storage limit was omitted.	The alternate-route service did not consistently define a non-zero ephemeralStorageLimit in custom values.yaml. Because the Helm template rendered limits.ephemeral-storage only when ephemeralStorageLimit was non-zero, the deployment skipped the ephemeral-storage limit for alternate-route. This resulted in alternate-route pods being deployed without an explicit ephemeral-storage limit. Doc Impact: There is no documentation impact.	3	26.1.200

Table 4-7 (Cont.) NRF 26.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
39688773	Incorrect ocLogId value and hop path in CDS logs under mixed traffic, breaking end-to-end traceability.	Under mixed duplicate-check and notification traffic, CDS logs showed an ocLogId and hop path that did not match the incoming request context. The asynchronous execution path did not consistently propagate the current request context, so duplicate-check traffic could appear as though it passed through Registration. This resulted in incorrect log correlation and reduced end-to-end traceability for CDS processing. Doc Impact: There is no documentation impact.	3	26.1.200
38850197	Access Token configuration validation response returned an incorrect parameter path for authConfig[1].serviceName.	NRF returned validation errors for the Access Token authentication feature with internal field names instead of public API parameter paths. Consequently, the validation response reported an incorrect parameter path for authConfig[1].serviceName, making it difficult to identify the invalid configuration in the submitted request. This affected only the validation error response and did not change the handling of valid Access Token configuration requests. Doc Impact: There is no documentation impact.	4	25.2.200
38974136	Old Ingress Gateway microservice pods underwent rolling restarts during same-release upgrades.	Old Ingress Gateway microservice pods were restarted unnecessarily during same-release Helm upgrades when globalIngressRateLimiting was enabled. Even when there were no changes to the deployment configuration or custom values.yaml, the deployment appeared modified because an internally generated hash value changed during each upgrade. This resulted in unnecessary rolling restarts of existing Ingress Gateway microservice pods during same-release upgrades even though no functional deployment changes had occurred. Doc Impact: There is no documentation impact.	4	24.1.3

Table 4-7 (Cont.) NRF 26.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38996646	NRF returned an incorrect maximumHopCount range message in the generalOptions REST API response.	NRF returned an incorrect validation message for maximumHopCount and maxSLFAttempts when invalid values were submitted through the REST API. Although the product accepted the documented boundary values, the error message described the supported range using exclusive boundaries. This resulted in a validation response that incorrectly implied valid boundary values were not supported and could mislead administrators during configuration. Doc Impact: There is no documentation impact.	4	25.2.200
39032189	NRF accepted an invalid slfConfigMode value in slfOptions.	NRF accepted and stored unsupported values for slfConfigMode in slfOptions, although the REST API supported only STATIC_SLF_CONFIG_MODE and DISCOVERED_SLF_CONFIG_MODE. This resulted in invalid configuration values being persisted instead of being rejected during configuration validation. Doc Impact: There is no documentation impact.	4	25.2.200
39442562	Grafana dashboard showed incorrect Egress Gateway microservice request rate.	The NRF Grafana dashboard showed incorrect Egress Gateway microservice request and response rate values because the PromQL queries did not consistently filter the metric by the expected egress direction. This resulted in the dashboard displaying incorrect or inconsistent Egress Gateway microservice rate values. Doc Impact: There is no documentation impact.	4	26.1.200

Table 4-7 (Cont.) NRF 26.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
39442597	NRF Grafana dashboard showed an incorrect SLF Query Success Ratio (2xx) percentage.	The NRF Grafana dashboard had an incorrect PromQL expression for the SLF Query Success Ratio (2xx) percentage panel. The denominator was filtered the same way as the 2xx numerator, so the panel calculated an incorrect success ratio. This resulted in the dashboard showing the wrong SLF success percentage. Doc Impact: There is no documentation impact.	4	26.1.200
39499880	False OcnrfHeapUsageCrossedMajorThreshold alarms were triggered for nrfauditor pods in production NRF.	Customer environments saw recurring OcnrfHeapUsageCrossedMajorThreshold alarms for nrfauditor pods even though the pods were stable, had no OOMKilled events, and showed no Java OutOfMemoryError. The alert thresholds were too aggressive for the expected nrfauditor heap usage pattern. This resulted in repeated false major heap alarms without any functional service impact. Doc Impact: There is no documentation impact.	4	25.1.203
39636137	NRF returned screening rules from all georedundant sites in the GET response.	The unfiltered screening-rules GET API returned screening-rule records from all sites in a three-site georedundant deployment instead of returning only the records owned by the local NRF instance. Replicated records from the other sites were included in the response. This resulted in the GET response returning screening-rule data outside the local site scope. Doc Impact: There is no documentation impact.	4	26.1.200

Note

Resolved bugs from 25.2.2xx have been forward ported to Release 26.1.201.

4.2.9 SEPP Resolved Bugs

Release 26.1.200

Table 4-8 SEPP 26.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
39176253	Missing https config in default sor peerset config	The default SOR peerset was created without HTTPS configuration while route metadata enforced httpsTargetOnly=true. This caused intermittent routing failures with "No https instances configured" and resulted in SOR regression failures. Doc Impact: There is no documentation impact.	2	25.2.200
39373350	SOR request from SEPP to SOR carries producer NF FQDN in header authority instead of configured SOR FQDN - v26.1.200	The SOR request used the producer NF FQDN in :authority instead of the configured SOR FQDN. Doc Impact: There is no documentation impact.	2	26.1.200
39476210	Hosted SEPP multi-FQDN feature not working in 26.1.200-rc.1	Hosted SEPP multi-FQDN functionality does not work. The handshake between the hosted SEPP and hosted partner is established successfully; however, the handshake between the roaming partner and hosted SEPP fails with a 401 Unauthorized error on hosted SEPP pn32c. Although the hosted SEPP multi-FQDN configuration is defined in custom_values.yaml, it is not reflected in the n32-ingress ConfigMap. As a result, the hosted SEPP multi-FQDN feature does not function as expected. Doc Impact: There is no documentation impact.	2	26.1.200

Table 4-8 (Cont.) SEPP 26.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
39656465	SEPP documentation updates required for EGW POP	In the SEPP Egress Gateway Pod Protection by Rate Limiting documentation, the User Guide, REST Guide, and Installation Guide contain inconsistent gateway names, REST URIs, Helm parameter names, and default values. Doc Impact: Updated the "Pod Protection By Rate Limiting" section in the <i>Oracle Communications Cloud Native Core Security Edge Protection Proxy User Guide</i>, <i>Oracle Communications Cloud Native Core Security Edge Protection Proxy REST Specification Guide</i> and updated the "Customizing SEPP" section in <i>Oracle Communications Cloud Native Core Security Edge Protection Proxy Installation, Upgrade, and Fault Recovery Guide</i>.	3	26.1.200
39707764	SEPP default YAML does not clearly expose seppPeerHealthCheck Codes for Proactive Health API.	SEPP Proactive Health API documentation suggesting seppPeerHealthCheckCodes may be configurable in custom-values.yaml, while only seppPeerHealthCheck is actually exposed. Doc Impact: Updated the healthyseppPeerHealthCheckCodes in the "Proactive Health API" section in the <i>Oracle Communications Cloud Native Core Security Edge Protection Proxy REST Specification Guide</i>.	3	26.1.200
39559658	Default error code profile mentioned in "Pod Protection by Rate Limiting" does not exist	The default error code profile referenced by Pod Protection Rate Limiting did not match the actual configured default error code profile available in the system. Doc Impact: Updated the "Error Code Profiles" section in the <i>Oracle Communications Cloud Native Core Security Edge Protection Proxy User Guide</i>.	3	26.1.200

Table 4-8 (Cont.) SEPP 26.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
39600267	SEPP-PERF:Duplicate includeClientCertIdentityAsTag parameter under n32-ingress-gateway causes intended metrics tagging configuration to be overridden in SEPP_26.1.200-rc.2	The includeClientCertIdentityAsTag parameter is configured twice in the same n32-ingress-gateway section with conflicting values. YAML parsing retains the last value, which sets the effective value to false. As a result, the ClientCertIdentity tag is not included in request and response metrics, although the earlier configuration enables it. Doc Impact: There is no documentation impact.	3	26.1.200
39694882	SEPP: oauthRequestValidation parameter missing from custom-values.yaml for OAuth get token request validation	The SEPP User Guide states that OAuth get-token request validation can be enabled by setting oauthRequestValidation: true under the Pn32f section in values.yaml. However, customers cannot modify the Helm chart values.yaml directly. Because the parameter is not exposed in custom-values.yaml, customers do not have a supported way to enable OAuth get-token request validation during deployment. Doc Impact: There is no documentation impact.	3	26.1.200
38257593	pn32f memory usage keep on increasing at 550 TPS with cat3 time check enabled	PN32F memory usage kept increasing during 550 TPS CAT3 time-check traffic because local NRF response caches were not released. Doc Impact: There is no documentation impact.	3	25.1.200
38278479	Getting "No https instances configured" intermittently in PLMN EGW logs	With NIF enabled, PLMN egress gateway intermittently logged internal routing errors during traffic, which indicated inconsistent HTTPS peer selection behavior and potential impact to stable NIF traffic routing. Doc Impact: There is no documentation impact.	3	25.1.201
38489579	SEPP sending extra TLS signature algorithms when it should limit what's being sent IAW SA-TLS-016	SEPP sent extra TLS signature algorithms beyond the SA-TLS-016 expected list. Doc Impact: There is no documentation impact.	3	25.1.200

Table 4-8 (Cont.) SEPP 26.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38943638	OCSEPP 25.1.202 Roaming Hub SEPP sending plmnIdList with null value in the n32c-handshake	During the handshake in 25.1.202, SEPP sent plmnIdList as null instead of sending it as an array, or omitting it when empty, as expected by 3GPP TS 29.573. Doc Impact: There is no documentation impact.	3	25.1.201
38989742	several standard and non-standard http headers are repeated when the request is being proxied by psepp to hSCP	Proxied requests repeated headers such as via, content-type, and user-agent. Doc Impact: There is no documentation impact.	3	25.2.200
39066880	SEPP: Wrong value of 'content-type' in response for Remote SEPP creation failure	Multiple Remote SEPP creation validation failures returned content-type: application/json instead of application/problem+json. Doc Impact: There is no documentation impact.	3	25.2.200
39074219	SEPP: Wrong value of 'content-type' in response for Remote SEPP set creation failure	Remote SEPP set creation failure responses returned application/json instead of application/problem+json. Doc Impact: There is no documentation impact.	3	25.2.200
39074274	Hosted SEPP: wrong error code is generated when Remote SEPP set is created with missing "hostedRemotePartnerSet" parameter	Creating a Remote SEPP set without hostedRemotePartnerSet returned a 500 Internal Server Error because of a null dereference, instead of the expected 4xx validation error. Doc Impact: There is no documentation impact.	3	25.2.200
39114099	errors being reported in sepp pn32f microservices	PN32F microservices reported Coherence/JMX and service-discovery errors in pod logs. Doc Impact: There is no documentation impact.	3	25.2.200
39126163	SEPP does not refuse a CONNECT method	SEPP did not immediately reject HTTP CONNECT method requests during screening tests and returned a 408 timeout instead. Doc Impact: There is no documentation impact.	3	25.1.201

Table 4-8 (Cont.) SEPP 26.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
39200159	Errors being reported in plmn egw and ARS microservice for NRF	PLMN egress gateway and Alternate Route Service reported NRF-related lookup errors when virtual NRF was deployed with the HTTP scheme. Doc Impact: There is no documentation impact.	3	25.2.200
39249940	SEPP: Hosted sepp removing via header of csepp during a Model-C service request	Hosted SEPP removed or missed the cSEPP via header during the Model-C service request flow. Doc Impact: There is no documentation impact.	3	25.2.200
39412205	ServiceDiscoveryException being reported in multiple SEPP services	Multiple SEPP services reported ServiceDiscoveryException from Kubernetes endpoint discovery failures. Doc Impact: There is no documentation impact.	3	26.1.200
39427362	SEPPConnectionFailureN32IGWAlert label not exposing error_reason label in the metric	The SEPPConnectionFailureN32IGWAlert metric did not expose the expected error_reason label. Doc Impact: There is no documentation impact.	3	25.1.201
39522482	PN32F Return 504 GATEWAY_TIMEOUT error with incorrect format	When PLMN egress gateway pods were down, PN32F returned an HTTP 504 Gateway Timeout response that did not use the required JSON Problem Details format. Doc Impact: There is no documentation impact.	3	25.1.203
39707787	Wrong formatting for seppPeerHealthCheckCodes in SEPP Proactive Health API documentation -26.1.200v	The User Guide incorrectly formats seppPeerHealthCheckCodes as healthyseppPeerHealthCheckCodes. Doc Impact: Updated "Proactive Health API" section in the <i>Oracle Communications Cloud Native Core Security Edge Protection Proxy User Guide</i> .	4	26.1.200

Table 4-8 (Cont.) SEPP 26.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
39728190	SEPP Installation Guide incorrectly lists n32 ingress gateway-only healthCheckMonitoring.enabled parameter under N32 Egress gateway - 26.1.200v	The Installation Guide incorrectly lists the ingress-only parameter n32-ingress-gateway.healthCheckMonitoring.enabled in the N32 Egress Gateway parameter table. This parameter is consumed only by the N32 Ingress Gateway chart and should be removed from the N32 Egress Gateway section. Doc Impact: Updated the "Customizing SEPP" section in the <i>Oracle Communications Cloud Native Core Security Edge Protection Proxy Installation, Upgrade, and Fault Recovery Guide</i> .	4	26.1.200
38484413	500 Internal Server Error logs in plmn egw logs during 1K traffic of NIF error copy	During 1K TPS NIF error-copy traffic, PLMN egress gateway generated 500 Internal Server Error logs, which potentially affected reliable error-copy processing at higher load. Doc Impact: There is no documentation impact.	4	25.2.100
38818844	SEPP-PERF: Refresh task failed due to invalid response code for k8s api query response at ocsepp-sepp-nrf-client-nfdiscovery & ocsepp-sepp-nrf-client-nfmanagement microservice during long performance run	During a long performance run, NRF client nfdiscovery and nfmanagement microservices logged refresh task failures because Kubernetes service discovery queries returned HTTP 403 responses. Doc Impact: There is no documentation impact.	4	25.2.100
39113794	SEPP: Missing dimensions in prometheus metric oc_egressgateway_connection_failure_total	The Prometheus metric oc_egressgateway_connection_failure_total missed the expected dimensions host, port, and errorReason that were documented in the user guide. Doc Impact: Updated oc_egressgateway_connection_failure_total metric dimensions in the <i>Oracle Communications Cloud Native Core Security Edge Protection Proxy User Guide</i> .	4	25.2.200

Table 4-8 (Cont.) SEPP 26.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
39211875	content-type is application/json when capability exchange fails	During N32-C capability exchange failure caused by PLMN list mismatch, SEPP returned a 400 Problem Details body with Content-Type: application/json instead of application/problem+json. Doc Impact: There is no documentation impact.	4	25.2.200
39410950	SEPP: custom yaml updates	The default custom YAML needed updates for atsSpecificDeployment and CNLB annotation examples. Doc Impact: The ocsepp_custom_values_<version>.yaml examples are updated in the in the <i>Oracle Communications Cloud Native Core Security Edge Protection Proxy Installation, Upgrade, and Fault Recovery Guide</i> .	4	26.1.200

Note

Resolved bugs from 25.2.201 have been forward-ported to Release 26.1.200

4.2.10 SCP Resolved Bugs

Release 26.1.201

Table 4-9 SCP 26.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
39660217	508 loop detected with HSS services	A 508 loop was detected with HSS services. Doc Impact: There is no documentation impact.	2	25.2.200
39567885	UpdateNotify not routed over TLS	SCP failed to route UpdateNotify to an SMF over TLS and returned a 504 error. Doc Impact: There is no documentation impact.	2	26.1.200
39385808	Notification routing issue	A notification routing issue occurred on SCP. Doc Impact: There is no documentation impact.	2	25.1.204

Table 4-9 (Cont.) SCP 26.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37886252	High-cardinality metrics and high memory consumption	High-cardinality metrics and high memory consumption were observed on SCP while traffic ran at full capacity. Doc Impact: There is no documentation impact.	2	25.1.100
39748785	UDV variables missing after an SCP upgrade from 25.2.203 to 26.1.201	UDV variables were missing after an SCP upgrade from 25.2.203 to 26.1.201. Doc Impact: There is no documentation impact.	3	26.1.200
39701340	Roaming notification traffic not routed through configured SEPP ports	Roaming notification traffic was not routed through the configured SEPP ports. Doc Impact: There is no documentation impact.	3	25.2.201
39569870	Connection failure before response timeout expiry	A connection failure occurred before the response timeout expired. Doc Impact: There is no documentation impact.	3	24.3.0
39616215	NF_PROFILES_UPDATE_HISTORY recorded NULL data for DEREGISTERED profiles after upgrade	NF_PROFILES_UPDATE_HISTORY recorded NULL data for DEREGISTERED profiles after an upgrade from 25.2.1xx. Doc Impact: There is no documentation impact.	3	26.1.200
39616210	ocscp_pod_overload_discard_by="PENDING_TRANSACTION" missing from a metric	The user guide did not document ocscp_pod_overload_discard_by="PENDING_TRANSACTION" for ocscp_worker_pod_overload_discard_req_total. Doc Impact: Updated the example of the "ocscp_worker_pod_overload_discard_req_total" metric in <i>Oracle Communications Cloud Native Core, Service Communication Proxy User Guide</i> .	3	26.1.200
39601835	SCPUnhealthyPeerSCPDetected alert not cleared	The SCPUnhealthyPeerSCPDetected alert did not clear as expected. Doc Impact: There is no documentation impact.	3	26.1.200

Table 4-9 (Cont.) SCP 26.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
39597102	Incorrect ocscp_nexthop_ocscp_fqdn dimension value	The SCP metrics documentation incorrectly identified the ocscp_nexthop_ocscp_fqdn dimension as ocscp_nexthop_scp_fqdn. Doc Impact: Updated the dimension of the "ocscp_metric_interscp_http_tx_req_total" and "ocscp_metric_interscp_http_rx_res_total" metrics in <i>Oracle Communications Cloud Native Core, Service Communication Proxy User Guide</i> .	3	26.1.200
39596149	Audit metric pegged for an empty successful NRF response	The audit metric was pegged when an empty successful response was received from NRF. Doc Impact: There is no documentation impact.	3	26.1.200
39581580	ocscp_metric_peer_scp_unhealthy_total not documented	The ocscp_metric_peer_scp_unhealthy_total metric was not documented in <i>Oracle Communications Cloud Native Core, Service Communication Proxy User Guide</i> . Doc Impact: Added the "ocscp_metric_peer_scp_unhealthy_total" metric in <i>Oracle Communications Cloud Native Core, Service Communication Proxy User Guide</i> .	3	26.1.200
39572859	authority header changed after an SCP upgrade	The authority header changed after an SCP upgrade to 25.1.202. Doc Impact: There is no documentation impact.	3	25.1.202
39571812	Ingress and egress metrics missing from the user guide	The SCP User Guide did not document ocscp_worker_ingress_req_total and ocscp_worker_egress_res_total. Doc Impact: Added the "ocscp_worker_ingress_req_total" and "ocscp_worker_egress_res_total" metrics in <i>Oracle Communications Cloud Native Core, Service Communication Proxy User Guide</i> .	3	26.1.200

Table 4-9 (Cont.) SCP 26.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
39520804	OCI for inter-SCP not working	OCI for inter-SCP did not work in SCP 25.2.203 Doc Impact: There is no documentation impact.	3	25.2.203
39503574	PUT method accepted empty nextHopRoamingProxyRoutingConfigData	The PUT method accepted empty nextHopRoamingProxyRoutingConfigData for the NextHopRoamingProxyRoutingConfig API. Doc Impact: There is no documentation impact.	3	25.2.200
39439839	Worker restarted during overload scenarios	SCP-Worker restarted during overload scenarios because of the liveness probe configuration. Doc Impact: There is no documentation impact.	3	26.1.200
39434020	Stale thread entries appeared in Thread Watch Dog information	Stale thread entries appeared in Thread Watch Dog information with COMPLETED+isStuck=true. Doc Impact: There is no documentation impact.	3	26.1.200
39394411	Invalid traffic-rejection parameter values did not return an error	SCP did not return an error for invalid retryAfter and redirect URL values in defaultScpTrafficRejectionErrorProfile in the CNC Console. Doc Impact: There is no documentation impact.	3	26.1.200
39367198	LCI Tx metrics dropped to zero after an upgrade	SCP LCI Tx metrics intermittently dropped to zero after an upgrade from 25.1.100 to 25.2.103. Doc Impact: There is no documentation impact.	3	25.2.103
39366469	Empty default values in defaultScpTrafficRejectionErrorProfile	The retryAfter and redirectURL default values were empty in defaultScpTrafficRejectionErrorProfile in the CNC Console. Doc Impact: There is no documentation impact.	3	26.1.200
39352037	Notification service did not process NF_PROFILE_CHANGED	An issue was observed in the SCP-Notification pod while processing NF profile change notifications received from NRF after a PATCH request on an NF instance. Doc Impact: There is no documentation impact.	3	25.1.203

Table 4-9 (Cont.) SCP 26.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
39329422	TLS handshake did not send the full certificate chain	SCP 25.1.202 could not be configured to send the full certificate chain in a TLS handshake. Doc Impact: There is no documentation impact.	3	25.1.202
39318652	Incorrect allowed values for reRouteConditionList	The CNC Console displayed incorrect allowed values for reRouteConditionList in Next Hop Proxy Routing Config. Doc Impact: There is no documentation impact.	3	26.1.200
39316730	Default port not added to a URI	The default port was not added to a URI when callBackUri did not specify an explicit port. Doc Impact: There is no documentation impact.	3	26.1.200
39308577	Incorrect reRouteConditionList values in the REST API Guide	The SCP REST API Guide listed incorrect default value and allowedRange values for reRouteConditionList in nextHopProxyRoutingConfig. Doc Impact: Corrected the default value and allowedRange for "reRouteConditionList" in <i>Oracle Communications Cloud Native Core, Service Communication Proxy REST Specification Guide</i> .	3	25.2.202
39251727	504 error for a UDR profile with an empty IPv4 address	SCP returned a 504 "Gateway Timeout" error when a UDR profile used an empty IPv4 address and the UDR profile instance ID and service instance ID were the same. Doc Impact: There is no documentation impact.	3	25.1.204
39244745	SCP profiles not updated with correct ports	SCP profiles were not updated with the correct ports. Doc Impact: There is no documentation impact.	3	25.2.102
39158867	SCPC subscription and notification Grafana panels not working	The SCPC-Subscription and SCPC-Notification Grafana panels did not work. Doc Impact: There is no documentation impact.	3	25.2.201

Table 4-9 (Cont.) SCP 26.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
39130117	ocscp_nf_type incorrectly pegged as SEPP	The ocscp_nf_type metric dimension was incorrectly pegged as SEPP for custom roaming proxy requests in ocscp_metric_http_ar_tx_req_total. Doc Impact: There is no documentation impact.	3	25.2.200
39123519	Incorrect discovery request type in a metric	The ocscp_worker_local_discovery_processing_time_total metric reported ocscp_nfdiscovery_req_type as MODEL_D_DELEG_DISC_REQ for Model-C discovery requests. Doc Impact: There is no documentation impact.	3	25.2.200
39107534	Upstream service time panel did not display values	The "SCP Upstream Service Time" Grafana panel did not display maximum, average, or current values. Doc Impact: There is no documentation impact.	3	25.2.200
39007898	Incorrect inter-SCP routing for default notifications	Inter-SCP routing was incorrect for default notifications for Model-C and Model-D. Doc Impact: There is no documentation impact.	3	25.1.200
38973405	ocscp_worker_transaction_time_exhausted_total did not peg reliably	The ocscp_worker_transaction_time_exhausted_total metric failed to peg randomly. Doc Impact: There is no documentation impact.	3	25.2.100
38964285	Complete budget allocated to the target API root header attempt	For a delayed discovery request with Timestamp Header enabled, the complete budget was allocated to the target-api-root header attempt. Doc Impact: There is no documentation impact.	3	25.2.200
38924939	ocscp_requester_nf_type reported as NA	The enhanced priority capacity metric reported ocscp_requester_nf_type as NA. Doc Impact: There is no documentation impact.	3	25.2.200

Table 4-9 (Cont.) SCP 26.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38920538	Different PATCH request behavior for roaming proxy NFs	After the NF_DEREGISTERED event, the producer NF profile remained in OCSCP_NW_TOPOLOGY_NF_PROFILES and could still be updated by patch requests during the grace period, whereas the custom roaming proxy profile was deleted and could not be updated. Doc Impact: There is no documentation impact.	3	25.2.200
38872318	PUT API response returned null timestamps	The PUT API response returned null timestamps. Doc Impact: There is no documentation impact.	3	25.2.200
38810553	Incorrect static NF discovery metric values	Static NF Discovery reported incorrect ocscp_nf_setid and ocscp_alternate_route_type values when the primary NF was unavailable. Doc Impact: There is no documentation impact.	3	25.2.200
38743406	SCPCacheQueuesUtilizationAboveCriticalThreshold alert raised	The SCPCacheQueuesUtilizationAboveCriticalThreshold alert was raised with 730K MPS and 1200 NF profiles. Doc Impact: There is no documentation impact.	3	25.2.100
38743377	SCPCoherenceCacheHitsRateAboveThreshold alert raised	The SCPCoherenceCacheHitsRateAboveThreshold alert was raised with 730K MPS and 1200 NF profiles. Doc Impact: There is no documentation impact.	3	25.2.100
38719001	Certificate-expiry metric and alert file required a rename	The ocscp_metric_ssl_certificate_expire_total metric and its alert file required a rename. Doc Impact: There is no documentation impact.	3	25.2.100
38444819	Mediation service updated a discovery target header only once	The SCP Mediation service updated the 3gpp-sbi-discovery-target-nf-type header only once when a mediation rule configured two updates. Doc Impact: There is no documentation impact.	3	25.2.100

Table 4-9 (Cont.) SCP 26.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38317992	Worker pod throttled egress traffic without a maximum concurrent stream	An SCP-Worker pod throttled egress traffic when the remote server did not send a maximum concurrent stream. Doc Impact: There is no documentation impact.	3	25.1.100
38209469	Exceptions occurred after an upgrade	Multiple exceptions occurred on worker and configuration pods after an upgrade. Doc Impact: There is no documentation impact.	3	25.1.200
38071919	Port not derived for ModelID Notification	The port was not derived from NFProfileLevelAttrConfig for ModelID Notification, and SCP used hardcoded port 80 for alternate routing. Doc Impact: There is no documentation impact.	3	25.1.200
37969345	Case-insensitive nfType handling in the topology source information REST API	The topologysourceinfo REST API did not handle nfType as case-sensitive. Doc Impact: Added information about nfType case sensitivity to the "Topology Source Info REST API" in <i>Oracle Communications Cloud Native Core, Service Communication Proxy REST Specification Guide</i> .	3	23.4.0
37554502	Worker pod restarted with overload errors	A newly spawned SCP worker pod restarted with overload errors after 25% or 50% of SCP worker pods entered a restart state. Doc Impact: There is no documentation impact.	3	25.1.100
39708559	RX_TX_MSG_INFO log level missing in the console GUI	The CNC console did not display the RX_TX_MSG_INFO log level. Doc Impact: There is no documentation impact.	4	26.1.200
39684540	retry-after header sometimes not honored	The retry-after header was sometimes not honored, and traffic was sent to the same NF. Doc Impact: There is no documentation impact.	4	25.2.203

Table 4-9 (Cont.) SCP 26.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
39597248	Incorrect allowed value for the redirectURL parameter	The SCP REST API Guide incorrectly listed "NA" as an allowed value for the redirectURL parameter. Doc Impact: Updated the allowed value of the "redirectURL" parameter in <i>Oracle Communications Cloud Native Core, Service Communication Proxy REST Specification Guide</i> .	4	26.1.200
39597052	ocscp_authority dimension appeared after disablement	The ocscp_authority dimension continued to appear in metrics after disablement. Doc Impact: Updated the description of the "ocscp_metric_http_rx_req_total" metric in <i>Oracle Communications Cloud Native Core, Service Communication Proxy User Guide</i> .	4	26.1.200
39590718	ocscp_cause values missing for rate-limiting-not-applied metrics	The ocscp_cause values were not documented for rate-limiting-not-applied metrics in <i>Oracle Communications Cloud Native Core, Service Communication Proxy User Guide</i> . Doc Impact: Added the "ocscp_cause" dimension in the "ocscp_metric_egress_rate_limiting_not_applied_req_total" and "ocscp_metric_ingress_rate_limiting_not_applied_req_total" metrics in <i>Oracle Communications Cloud Native Core, Service Communication Proxy User Guide</i> .	4	26.1.200
39581566	Incorrect metric parameter example	The user guide included an incorrect metric parameter example. Doc Impact: Updated the example of the "ocscp_metric_egress_rate_limiting_not_applied_req_total" metric in <i>Oracle Communications Cloud Native Core, Service Communication Proxy User Guide</i> .	4	26.1.200
39476699	Egress congestion control did not throttle traffic	SCP did not throttle traffic for egress congestion control. Doc Impact: There is no documentation impact.	4	25.2.102

Table 4-9 (Cont.) SCP 26.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
39436160	ocscp_metric_scp_generated_response_total pegged twice	The ocscp_metric_scp_generated_response_total metric was pegged twice because of a race condition between the normal termination path and total transaction timeout. Doc Impact: There is no documentation impact.	4	26.1.200
39417794	ocscp_fqdn missing from a deregistration metric	The user guide did not document ocscp_fqdn for ocscp_subscription_nrf_deregistration_success_total. Doc Impact: Added "ocscp_fqdn" to the "ocscp_subscription_nrf_deregistration_success_total" metric dimension and example in <i>Oracle Communications Cloud Native Core, Service Communication Proxy User Guide</i> .	4	26.1.200
39392109	Alarm OID query issue	An alarm OID query issue occurred. Doc Impact: There is no documentation impact.	4	25.2.102
39107451	Requester NF type list option returned an error	The "*" option in the CNCC GUI returned an error for Requester NF Type List in NF Discovery Mode Config. Doc Impact: There is no documentation impact.	4	25.2.200
38962325	Incomplete validation message for discovery mode fallback criteria	The validation message for Discovery Mode Fallback Criteria did not list the supported connectionError and timeout options. Doc Impact: There is no documentation impact.	4	25.2.200
38947469	Incorrect error cause for a missing mandatory API parameter	SCP returned an incorrect error cause when a mandatory parameter was missing in a Proxy Selection Routing Mode API request. Doc Impact: There is no documentation impact.	4	25.2.200

Table 4-9 (Cont.) SCP 26.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38930373	Incorrect error cause for an invalid congestion-control configuration value	SCP returned an incorrect error cause when nextHopProxyNfServiceData.nfServiceLoadBasedCongestionControlCfg had an invalid value. Doc Impact: There is no documentation impact.	4	25.2.200
39504439	ocscp_locality is missing in ocscp_metric_scp_generated_response_total of user guide.	The SCP user guide does not document the ocscp_locality for ocscp_metric_scp_generated_response_total metric. Doc Impact: Added the missing "ocscp_locality" dimension for the "ocscp_metric_scp_generated_response_total" metric in <i>Oracle Communications Cloud Native Core, Service Communication Proxy User Guide</i> .	4	26.1.200
38815291	Enhanced Consumer NF Selection Info Auto-Selected Causes 400 Error During NF Selection Mode Update.	Auto-selecting Enhanced Consumer NF Selection Info causes a 400 error during an NF Selection Mode update. Doc Impact: Updated NF Selection Mode documentation for Enhanced Consumer NF Selection configuration in the "CNC Console" section in <i>Oracle Communications Cloud Native Core, Service Communication Proxy User Guide</i> .	4	25.2.200
38395424	Missing and Incorrect Parameters in Official SCP Documentation	Some of the Helm parameters were missing from the <i>Oracle Communications Cloud Native Core, Service Communication Proxy Installation, Upgrade, and Fault Recovery Guide</i> . Doc Impact: Added the missing Helm parameters in the "Global Parameters" section in <i>Oracle Communications Cloud Native Core, Service Communication Proxy Installation, Upgrade, and Fault Recovery Guide</i> .	4	25.2.100

Note

Resolved bugs from 25.2.100, 25.2.204, and 26.1.200 have been forward ported to Release 26.1.201.

Release 26.1.201

Table 4-10 SCP ATS 26.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
39680503	SCP0015 WS1.5 full regression failed	The metric validation failed for <code>ocscp_metric_ingress_rate_limiting_not_applied_req_total</code> . Doc Impact: There is no documentation impact.	3	25.2.203
39108180	NF Profile Configuration PUT API did not return a response	The NF Profile Configuration PUT REST API did not return a response when the profile was successfully registered or updated. Doc Impact: There is no documentation impact.	3	26.1.200

Note

Resolved bugs from 25.2.2xx and 26.1.200 have been forward ported to Release 26.1.201.

4.2.11 Common Services Resolved Bugs

4.2.11.1 Egress Gateway Resolved Bugs

Release 26.1.201

Table 4-11 Egress Gateway 26.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37696738	IRC exceptions are not updating in Grafana or Prometheus only in the PODs logs its updated	IRC exceptions were logged in pods but were not reflected in Grafana or Prometheus for <code>http_server_requests_seconds_count</code> and <code>oc_ingressgateway_http_responses_total</code> . Doc Impact There is no documentation impact.	3	25.1.100
38953545	"jetty parameter <code>MaxResponseHeadersSize</code> " boundary check is missing	The boundary validation for <code>jettyMaxResponseHeadersSize</code> was missing, allowing an installation to complete while Ingress Gateway entered <code>CrashLoopBackOff</code> . Doc Impact There is no documentation impact.	3	26.1.200

Table 4-11 (Cont.) Egress Gateway 26.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
39162947	Changing serviceMeshEnabled using setter method is not changing the serviceDiscoveryMechanism	Changing serviceMeshEnabled through its setter did not update serviceDiscoveryMechanism. Doc Impact There is no documentation impact.	2	26.1.200
39181670	None of the Grafana Panels are updating in the Latest OCCNE Cluster(25.2.200)	Grafana panels did not update with the latest Ingress Gateway traffic, latency, memory, and CPU results on 25.2.200. Doc Impact There is no documentation impact.	3	26.1.200
39083890	EGW logs for message "HTTP response body is empty" doesn't contain ocLogId	Egress Gateway logs for the "HTTP response body is empty" message did not contain ocLogId, preventing ocLogId-based log filtering. Doc Impact There is no documentation impact.	3	25.2.108
39154470	SBI Service Operations CNCC screen is not allowing to save modified entry	The SBI Service Operations screen did not save a configuration with a blank initiatedRequestPriorityRule or responsePriorityRule and returned HTTP 400 CFG-E107. Doc Impact There is no documentation impact.	3	26.1.200

Note

Resolved bugs from 25.1.200 have been forward ported to Release 26.1.201.

Release 26.1.200**Table 4-12 Egress Gateway 26.1.200 Resolved Bugs**

Bug Number	Title	Description	Severity	Found in Release
38522842	First lookup call to ARS is failing for configured vFQDN	The initial Alternate Route Service lookup for a configured vFQDN failed, although subsequent lookups succeeded. Doc Impact: There is no documentation impact.	3	25.1.203

Table 4-12 (Cont.) Egress Gateway 26.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38405814	Post_rollback_SM_Validation fails at alternate-route logging level validation	After the rollback, system-manager validation failed while validating the Alternate Route Service logging level. Doc Impact: There is no documentation impact.	3	25.2.100
38997505	Unformatted WARN log "WARN found 2 argument placeholders, but provided 3 for pattern " is seen inpre-upgrade hook logs of alternate route, ingress-gw and egress-gw	The preupgrade hooks logged an unformatted WARN message because the placeholder count did not match the supplied arguments. Doc Impact: There is no documentation impact.	4	26.1.200
38513360	IGW/EGW/ARS Deployment YAML having both "replicas" and "minReplicas/maxReplicas"	The deployment YAML file included both replicas and minReplicas/maxReplicas settings. Doc Impact: There is no documentation impact.	3	25.1.205
39060179	Upgrade to 26.1.2xx fails at nrf-client-nfdiscovery-pre-upgrade hook	The upgrade to Gateway Services 26.1.2xx failed in the nrf-client-nfdiscovery pre-upgrade hook. Doc Impact: There is no documentation impact.	2	25.2.200
38461465	Sender Attribute should only consist SEPP-<sepp-fqdn> when additional error logging in enabled in gw logging config	When additional error logging was enabled, the Gateway Services sender attribute was incorrectly populated. Doc Impact: There is no documentation impact.	4	25.2.100
39043146	Common-config-hook 26.1.200-rc.3 giving APPLICATION FAILED TO START error in app-info microservice hooks	The common-config hook caused the app-info microservice hooks to fail with an application-start error. Doc Impact: There is no documentation impact.	3	26.1.200
39061499	Common-Config: Alter Command not allowed	Common Config did not allow the required ALTER command. Doc Impact: There is no documentation impact.	2	26.1.200

Table 4-12 (Cont.) Egress Gateway 26.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38246506	When EGW request for the "defaultNRFInstance" then "oc_oauth_nrf_request_total" metric is not updated	Egress Gateway did not update the oc_oauth_nrf_request_total metric when it requested defaultNRFInstance. Doc Impact: There is no documentation impact.	3	25.2.100
38179718	In oc_egressgateway_http_responses_total metric NFTYPE should be corrected and No traffic drop observed	The oc_egressgateway_http_responses_total metric reported an incorrect NF type. Doc Impact: There is no documentation impact.	4	24.2.15
38235950	NPE seen in egress gateway after pod restart	Egress Gateway logged a NullPointerException after its pods restarted. Doc Impact: There is no documentation impact.	3	25.2.100
38551540	Call rejected with Status 0 in EGW 25.2.200-rc.1 build.	Egress Gateway rejected calls with status 0. Doc Impact: There is no documentation impact.	3	25.2.200-rc.1
38585721	High CPU and Memory usage in EGW 25.2.200-rc.1 build as compared with previous build 25.2.100.	Egress Gateway used significantly more CPU and memory than the previous build. Doc Impact: There is no documentation impact.	2	25.2.200
38596250	404 NOT_FOUND ERROR and traffic failure observed at EGW	Egress Gateway returned 404 NOT_FOUND responses and caused traffic failures. Doc Impact: There is no documentation impact.	3	25.2.200
38433760	EGW is sending data packets followed by header with some delay resulting which calls are failing.	Egress Gateway sent data packets before their headers, with a delay that caused calls to fail. Doc Impact: There is no documentation impact.	2	25.2.200

Table 4-12 (Cont.) Egress Gateway 26.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38644699	TTL value in lookup is showing greater than the value defined in DNS SRV records in ARS 25.2.200-rc.1	Alternate Route Service reported a DNS lookup TTL greater than the TTL configured in DNS SRV records. Doc Impact: There is no documentation impact.	2	25.2.200-rc.1
38575922	Inclusion of Configurable flags to enable/disable addition of X-Forwarded headers by SCG in EGW values.yaml	Egress Gateway's values.yaml file did not provide attributes to control SCG addition of X-Forwarded headers. Doc Impact: There is no documentation impact.	3	25.2.200-rc.1
38702789	Peer health ping request getting timed out when EGW is freshly installed/ upgraded in dual stack with IPv6 address	Peer-health ping requests timed out after a fresh installation or upgrade in dual-stack IPv6 deployments. Doc Impact: There is no documentation impact.	2	25.1.207
38661262	HealthStatus/peerSet GET, giving 500 , NULL POINTER EXCEPTION in response	The HealthStatus/peerSet GET request returned HTTP 500 with a NullPointerException. Doc Impact: There is no documentation impact.	2	25.2.200
38434182	Policy upgrade failing due to EGW failed to connect to database while upgrading from 25.1.200 to 25.2.101-rc.1	A Policy upgrade failed because Egress Gateway could not connect to the database. Doc Impact: There is no documentation impact.	3	25.2.101
38828633	Scheme change for the same host:port was not handled correctly during concurrent updates	Concurrent updates did not correctly handle a scheme change for the same host and port. Doc Impact: There is no documentation impact.	3	25.2.106
38515750	EGW not validating the LCI configure parameter loadThreshold present or not	Egress Gateway did not validate whether the LCI loadThreshold parameter was present. Doc Impact: There is no documentation impact.	4	25.2.102

Table 4-12 (Cont.) Egress Gateway 26.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38522816	EGW fails to build peer health table after initial ARS call fails	Egress Gateway did not build the peer-health table when the initial Alternate Route Service call failed. Doc Impact: There is no documentation impact.	3	25.1.203
38719525	peer health status is showing incorrect peer scheme for https peer in EGW 25.2.105 build	Egress Gateway reported an incorrect peer scheme for HTTPS peers. Doc Impact: There is no documentation impact.	2	25.2.105
38795596	During EGW Upgrade from 25.1.203 to 25.2.106 Observed "java.io.InvalidClassException" on new 25.2.106 egw pods and No traffic drop observed.	Egress Gateway pods logged java.io.InvalidClassException during the upgrade. Doc Impact: There is no documentation impact.	3	25.2.106
38901642	PCF using expired token (26.1.200)	PCF used an expired token. Doc Impact: There is no documentation impact.	2	25.2.106
38902573	Newly Updated DNS entries are not updating to EGW peer health table	Newly updated DNS entries were not reflected in the Egress Gateway peer-health table. Doc Impact: There is no documentation impact.	2	26.1.200
38704688	EGW peer health status is inconsistent in case of multiple EGW pods in IPv6 with a synchronization delay of ~>=1min	Multiple Egress Gateway pods reported inconsistent peer-health status in IPv6 deployments after a synchronization delay. Doc Impact: There is no documentation impact.	2	25.1.207
38537310	Getting Intermittent error logs on PLMN EGW while running traffic	PLMN Egress Gateway generated intermittent error logs while traffic was running. Doc Impact: There is no documentation impact.	3	25.1.201

Table 4-12 (Cont.) Egress Gateway 26.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38856622	EGW - Error Response enhancement validation failing when All peers are Unhealthy	Egress Gateway error-response enhancement validation failed when every peer was unhealthy. Doc Impact: There is no documentation impact.	3	26.1.200
38661597	Metric oc_egressgateway_peer_health_status showing incorrect peer status in EGW 25.1.207-beta.1/25.2.106 build.	The oc_egressgateway_peer_health_status metric reported incorrect peer status. Doc Impact: There is no documentation impact.	3	25.1.206
38894990	PCF EGW not giving precedence to IPV6 and resolving to IPV4 address	PCF Egress Gateway resolved IPv4 addresses instead of preferring IPv6 addresses. Doc Impact: There is no documentation impact.	3	25.1.203
38957729	EGW is not able to send access token request towards NRF in TLS enabled setup.	Egress Gateway could not send access-token requests to NRF in a TLS-enabled deployment. Doc Impact: There is no documentation impact.	2	25.1.208
38902994	Peer Monitoring feature not working	The peer-monitoring feature did not work. Doc Impact: There is no documentation impact.	2	26.1.200
39049489	EGW 26.1.200-rc.3: EGW not giving precedence to IPv6 while initiating the connection towards NRF(Oauth) and Producer perfgo with IPv6_IPv4 based deployment in dual stack supported cluster.	Egress Gateway did not prefer IPv6 when connecting to NRF or to the producer in a dual-stack deployment. Doc Impact: There is no documentation impact.	2	26.1.200
38066375	Gateway is returning incorrect error when the cause is final request timeout is <=0	Gateway Services returned an incorrect error when the final request timeout was less than or equal to zero. Doc Impact: There is no documentation impact.	4	25.1.201

Table 4-12 (Cont.) Egress Gateway 26.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38998368	EGW pods are restarting while running traffic	Egress Gateway pods restarted while processing traffic. Doc Impact: There is no documentation impact.	2	25.2.108
38239527	For status code "404 " oc_egressgateway_http_responses_total metrics are not updated	The oc_egressgateway_http_responses_total metric was not updated for HTTP 404 responses. Doc Impact: There is no documentation impact.	3	25.2.100
39074445	Traffic failure on EGW when x-http2-scheme is added in GlobalRequestRemoveHeader	Egress Gateway traffic failed when x-http2-scheme was configured for request-header removal. Doc Impact: There is no documentation impact.	2	26.1.200
38902440	EGW is not removing headers present in globalRemoveRequestHeader and removeRequestHeader at Global and route level when forwarding the request towards Server	Egress Gateway did not remove configured global and route-level request headers before forwarding requests. Doc Impact: There is no documentation impact.	2	26.1.200
36891476	Default "expiry_in" timer should be configured in EGW for access token	Egress Gateway did not configure a default expiry_in timer for access tokens. Doc Impact: There is no documentation impact.	3	24.2.5
38257511	For "Expire_in" zero value EGW always taking token from Cache. after this scenario EGW will not send any request to NRF	When expiry_in was zero, Egress Gateway always used the cached token and stopped sending token requests to NRF. Doc Impact: There is no documentation impact.	3	25.2.100
38920277	EGW default custom yaml has duplicate keys.	The default Egress Gateway custom-values.yaml file contained duplicate keys. Doc Impact: There is no documentation impact.	3	26.1.200

Table 4-12 (Cont.) Egress Gateway 26.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
39148753	Metric 'oc_cnc_jetty_connections_active' pegged in EGW for both intraNF and interNF connections in 26.1.200-rc.4.	The oc_cnc_jetty_connections_active metric remained pegged for intra-NF and inter-NF connections. Doc Impact: There is no documentation impact.	3	26.1.200
39062313	3Gpp-Sbi-Lci header is not being sent out from EGW	Egress Gateway did not send the 3Gpp-Sbi-Lci header. Doc Impact: There is no documentation impact.	3	26.1.200
38592367	CNC - jetty : Boundary values are not Validated in the newly introduced and old parameters.	CNC Jetty did not validate boundary values for new and existing parameters. Doc Impact: There is no documentation impact.	3	25.2.200-rc.1
38552272	EGW rejects requests when enableOutgoingHTTP1 is enabled and the oc-http-version: http1 header is present.	Egress Gateway rejected requests when outgoing HTTP/1 was enabled and the HTTP/1 version header was present. Doc Impact: There is no documentation impact.	2	25.2.200
38504941	EGW/IGW should include LCI header when the current load is less than or equals to the difference between previously reported load and configured LoadThreshold value	Egress Gateway and Ingress Gateway did not include the LCI header when the load-threshold condition was met. Doc Impact: There is no documentation impact.	3	25.2.102
38789763	IGW/EGW Pods are not coming up when localLciHeaderValidity is assigned with value 14400000, under lciheaderconfig	Ingress Gateway and Egress Gateway pods did not start when localLciHeaderValidity was set to 14400000. Doc Impact: There is no documentation impact.	3	25.2.106

Table 4-12 (Cont.) Egress Gateway 26.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38818360	ASM : helm install is failing with execution error at "custom-header.tpl:3:3): defaultVal is null" and same working fine in the 25.1.207 build	ASM Helm installation failed because custom-header.tpl received a null default value. Doc Impact: There is no documentation impact.	2	25.2.106
38460669	Requesting APIGW to provide a metric which give NFs the end to end latency	APIGW did not provide a metric for end-to-end NF latency. Doc Impact: There is no documentation impact.	Requesting APIGW to provide a metric which give NFs the end to end latency	25.2.101
38828770	/nf-common-component/v1/igw/applicationparams API is returning multiple entries during Policy NF upgrade causing pod resrarts on audit service of PCF	The applicationparams API returned multiple entries during a Policy NF upgrade, causing audit-service pods to restart. Doc Impact: There is no documentation impact.	3	25.2.106
38861854	Increase of failure rate % after in service upgrade to 24.2.4 and to 25.1.202	The traffic failure rate increased after in-service upgrades. Doc Impact: There is no documentation impact.	2	24.2.13
38992190	prioritymappingrules accepts invalid received range format without validation	prioritymappingrules accepted an invalid received-range format without validation. Doc Impact: There is no documentation impact.	3	26.1.200
38992126	prioritymappingrules allows leading-zero values for received/used, causing ambiguous/ duplicate priority mappings	prioritymappingrules accepted leading-zero priority values, producing ambiguous or duplicate mappings. Doc Impact: There is no documentation impact.	4	26.1.200

Table 4-12 (Cont.) Egress Gateway 26.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38991946	prioritymappingrules validation rejects used as non-integer but rule-level detail is missing	prioritymappingrules rejected a non-integer used value without identifying the affected rule. Doc Impact: There is no documentation impact.	4	26.1.200
38992098	prioritymappingrules accepts duplicate received key within a rule object; last value silently overrides earlier value (last-key-wins)	prioritymappingrules accepted duplicate received keys within one rule and silently used the last value. Doc Impact: There is no documentation impact.	3	26.1.200
38992014	prioritymappingrules request with duplicate rules key is accepted; earlier rules array is silently overwritten (last-key-wins)	prioritymappingrules accepted duplicate rules keys and silently overwrote the earlier rules array. Doc Impact: There is no documentation impact.	3	26.1.200
38991138	PUT global-configuration/sbIServiceOperations behaves inconsistently with duplicate sbiServiceOperation keys (order-dependent)	The sbIServiceOperations PUT request handled duplicate sbiServiceOperation keys inconsistently based on their order. Doc Impact: There is no documentation impact.	3	26.1.200
38645273	Signature schemes in certificate request message TLS contains "not supported" values	TLS certificate-request messages included unsupported signature schemes. Doc Impact: There is no documentation impact.	3	25.1.200
38953545	jetty parameter MaxResponseHeadersSize boundary check is missing	The non-ASM Jetty MaxResponseHeadersSize parameter did not have boundary validation. Doc Impact: There is no documentation impact.	3	26.1.200

Table 4-12 (Cont.) Egress Gateway 26.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
39108214	IGW/EGW is not applying default rule while processing SMP Header request even when requestsmphheaders table in CCG is null.	Ingress Gateway and Egress Gateway did not apply the default rule to SMP-header requests when the requestsmphheaders table was null. Doc Impact: There is no documentation impact.	2	26.1.200
39009617	common_configuration_global table is getting updated even though applyHelmConfigOnUpgrade is set to false with HELM upgrade.	A Helm upgrade updated common_configuration_global even when applyHelmConfigOnUpgrade was false. Doc Impact: There is no documentation impact.	2	26.1.200
38943732	During upgrade and Rollback from 25.2.107 to 26.1.200-rc1 32% and 47%traffic loss observed.	Upgrade and rollback caused substantial traffic loss. Doc Impact: There is no documentation impact.	2	26.1.200
39028063	ASM:wrong error detail when helm upgraded with Pseudo range values in priority mapping rule configuration	An ASM Helm upgrade returned incorrect error details for pseudo-range priority-mapping values. Doc Impact: There is no documentation impact.	3	26.1.200
39005829	requestsmphheaders duplicate validation is case-sensitive	requestsmphheaders duplicate validation was case-sensitive. Doc Impact: There is no documentation impact.	4	26.1.200
39020622	No Input Validation on requestsmphheaders PUT Endpoint	The requestsmphheaders PUT endpoint did not validate input. Doc Impact: There is no documentation impact.	2	26.1.200
39033197	ASM:Error description for HELM upgrade failure and REST base upgrade failure should be in sync	Helm and REST-based upgrades returned inconsistent error descriptions for the same failure. Doc Impact: There is no documentation impact.	3	26.1.200

Table 4-12 (Cont.) Egress Gateway 26.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
39031628	Not allowing sbiserviceoperations to be configured without initiatedRequestPriorityRule and responsePriorityRule key parameters using HELM install/upgrade	Helm installation and upgrade did not allow sbiserviceoperations to be configured without its priority-rule keys. Doc Impact: There is no documentation impact.	3	26.1.200
39046579	Outgoing message missing defaultSmpHeaderName name when incoming 3gpp-sbi-message-priority header value is out of range	Outgoing messages omitted defaultSmpHeaderName when the incoming message-priority value was out of range. Doc Impact: There is no documentation impact.	3	26.1.200
39155503	Wrong error message is sent in response when initiatedRequestPriorityRule or responsePriorityRule are empty or null	The response returned an incorrect error message when either priority rule was empty or null. Doc Impact: There is no documentation impact.	3	26.1.200
39154470	SBI Service Operations CNCC screen is not allowing to save modified entry	The SBI Service Operations CNC Console screen did not allow a modified entry to be saved. Doc Impact: There is no documentation impact.	3	26.1.200
38974389	To provide updated Grafana json wrt Spring Boot to 3.2.x upgrade changes for both IGW and EGW.	Grafana JSON was not updated for the Spring Boot 3.2.x changes. Doc Impact: There is no documentation impact.	3	26.1.200
39128713	no match route exception from egress gateway.	Egress Gateway returned a no-match-route exception. Doc Impact: There is no documentation impact.	2	26.1.200
38992215	prioritymappingrules inconsistent validation/error messaging for defaultSmpHeaderName when empty string vs null	prioritymappingrules handled an empty defaultSmpHeaderName inconsistently with a null value. Doc Impact: There is no documentation impact.	4	26.1.200

Table 4-12 (Cont.) Egress Gateway 26.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38162347	for Custom Header request using REST-API, the complete array is not getting validated	REST API validation for custom-header requests did not validate the entire array. Doc Impact: There is no documentation impact.	3	25.1.203
36820640	Error Detail response for common config is not having Servicename and AppErrorCode in Error detail	Common Config error-detail responses omitted the service name and application error code. Doc Impact: There is no documentation impact.	3	24.2.4
35505051	Custom Package logging support for IGW & EGW	Ingress Gateway and Egress Gateway did not support custom-package logging. Doc Impact: There is no documentation impact.	3	23.2.0
38271114	Gateway configuration rollback does not work using FluxCD when it upgrades to a version it was deployed earlier	FluxCD could not roll back Gateway Services configuration to a version that had previously been deployed. Doc Impact: There is no documentation impact.	3	NA
37914904	Required Grafana dashboard JSON containing all the metrics for PI-B-25 PoP25 feature (IGW+EGW) along with Traffic success	The required Grafana dashboard JSON did not include all relevant metrics and traffic-success information. Doc Impact: There is no documentation impact.	4	25.1.200
34920448	NRF-Incorrect API gives 200 OK and creating config entry in DB for altRoute/logging	An invalid NRF API request returned HTTP 200 and created a configuration entry in the database. Doc Impact: There is no documentation impact.	4	22.2.0
38324716	Mounting of secrets is not backward compatible approach	Secret mounting was not backward compatible. Doc Impact: There is no documentation impact.	3	25.1.200

Table 4-12 (Cont.) Egress Gateway 26.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38611657	CNCC Ingress Gateway 500 â€œ reqHeaders null at CnccAuthorizationUtil.setRequestAttributes	The Spring Boot uplift caused Ingress Gateway to throw a null reqHeaders exception in CnccAuthorizationUtil.setRequestAttributes. Doc Impact: There is no documentation impact.	3	25.2.200
38827897	cnc_jetty_service_discovery metrics incorrectly pegged with value zero in ASM deployment	In ASM deployments, the cnc_jetty_service_discovery metrics incorrectly remained at 0. Doc Impact: There is no documentation impact.	3	25.2.200

Note

Resolved bugs from 25.1.200 have been forward ported to Release 26.1.200.

4.2.11.2 Ingress Gateway Resolved Bugs

Release 26.1.201**Table 4-13 Ingress Gateway 26.1.201 Resolved Bugs**

Bug Number	Title	Description	Severity	Found in Release
37696738	IRC exceptions are not updating in Grafana or Prometheus only in the PODs logs its updated	IRC exceptions were logged in pods but were not reflected in Grafana or Prometheus for http_server_requests_seconds_count and oc_ingressgateway_http_responses_total. Doc Impact There is no documentation impact.	3	25.1.100
38953545	"jetty parameter MaxResponseHeadersSize" boundary check is missing	The boundary validation for jettyMaxResponseHeadersSize was missing, allowing an installation to complete while Ingress Gateway entered CrashLoopBackOff. Doc Impact There is no documentation impact.	3	26.1.200

Table 4-13 (Cont.) Ingress Gateway 26.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
39162947	Changing serviceMeshEnabled using setter method is not changing the serviceDiscoveryMechanism	Changing serviceMeshEnabled through its setter did not update serviceDiscoveryMechanism. Doc Impact There is no documentation impact.	2	26.1.200
39181670	None of the Grafana Panels are updating in the Latest OCCNE Cluster(25.2.200)	Grafana panels did not update with the latest Ingress Gateway traffic, latency, memory, and CPU results on 25.2.200. Doc Impact There is no documentation impact.	3	26.1.200
39083890	EGW logs for message "HTTP response body is empty" doesn't contain ocLogId	Egress Gateway logs for the "HTTP response body is empty" message did not contain ocLogId, preventing ocLogId-based log filtering. Doc Impact There is no documentation impact.	3	25.2.108
39178062	IGW rejecting accesstoken requests with 503 backend not able to handle traffic	Ingress Gateway rejected access-token requests with HTTP 503 under discovery traffic because requests were not sent to the access-token back end. Doc Impact There is no documentation impact.	2	26.1.200
39158501	In IGW:26.1.200 the functionality of Content-Length and Content-Type headers are not working properly	Ingress Gateway incorrectly appended Content-Type: application/octet-stream and handled Content-Length inconsistently for empty POST requests. Doc Impact There is no documentation impact.	2	26.1.200
39171586	Cause "OAuth access Token is not present at IGW" error "oc_ingressgateway_http_requests_total" metrics are not updated & "oc_ingressgateway_http_responses_total" updated	For the HTTP 401 "OAuth access Token is not present at IGW" error, oc_ingressgateway_http_requests_total was not updated while oc_ingressgateway_http_responses_total was updated. Doc Impact There is no documentation impact.	3	26.1.200
39170610	Incorrect Request Count Metric oc_ingressgateway_http_requests_total – Underreporting Total Requests at Pod Level	oc_ingressgateway_http_requests_total significantly under-reported requests received by the pod compared with back-end request counts. Doc Impact There is no documentation impact.	3	26.1.200

Table 4-13 (Cont.) Ingress Gateway 26.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
39154470	SBI Service Operations CNCC screen is not allowing to save modified entry	The SBI Service Operations screen did not save a configuration with a blank <code>initiatedRequestPriorityRule</code> or <code>responsePriorityRule</code> and returned HTTP 400 CFG-E107. Doc Impact: There is no documentation impact.	3	26.1.200

Note

Resolved bugs from 25.1.200 have been forward ported to Release 26.1.201.

Release 26.1.200

Table 4-14 Ingress Gateway 26.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38522842	First lookup call to ARS is failing for configured vFQDN	The initial Alternate Route Service lookup for a configured vFQDN failed, although subsequent lookups succeeded. Doc Impact: There is no documentation impact.	3	25.1.203
38405814	Post_rollback_SM_Validation fails at alternate-route logging level validation	After the rollback, system-manager validation failed while validating the Alternate Route Service logging level. Doc Impact: There is no documentation impact.	3	25.2.100
38997505	Unformatted WARN log "WARN found 2 argument placeholders, but provided 3 for pattern " is seen in pre-upgrade hook logs of alternate route, ingress-gw and egress-gw	The preupgrade hooks logged an unformatted WARN message because the placeholder count did not match the supplied arguments. Doc Impact: There is no documentation impact.	4	26.1.200

Table 4-14 (Cont.) Ingress Gateway 26.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38513360	IGW/EGW/ARS Deployment YAML having both "replicas" and "minReplicas/maxReplicas"	The deployment YAML file included both replicas and minReplicas/maxReplicas settings. Doc Impact: There is no documentation impact.	3	25.1.205
39060179	Upgrade to 26.1.2xx fails at nrf-client-nfdiscovery-pre-upgrade hook	The upgrade to Gateway Services 26.1.2xx failed in the nrf-client-nfdiscovery pre-upgrade hook. Doc Impact: There is no documentation impact.	2	25.2.200
38461465	Sender Attribute should only consist SEPP-<sepp-fqdn> when additional error logging in enabled in gw logging config	When additional error logging was enabled, the Gateway Services sender attribute was incorrectly populated. Doc Impact: There is no documentation impact.	4	25.2.100
39043146	Common-config-hook 26.1.200-rc.3 giving APPLICATION FAILED TO START error in app-info microservice hooks	The common-config hook caused the app-info microservice hooks to fail with an application-start error. Doc Impact: There is no documentation impact.	3	26.1.200
39061499	Common-Config: Alter Command not allowed	Common Config did not allow the required ALTER command. Doc Impact: There is no documentation impact.	2	26.1.200
38592367	CNC - jetty : Boundary values are not Validated in the newly introduced and old parameters.	CNC Jetty did not validate boundary values for new and existing parameters. Doc Impact: There is no documentation impact.	3	25.2.200-rc.1

Table 4-14 (Cont.) Ingress Gateway 26.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38552272	EGW rejects requests when enableOutgoingHTTP1 is enabled and the oc-http-version: http1 header is present.	Egress Gateway rejected requests when outgoing HTTP/1 was enabled and the HTTP/1 version header was present. Doc Impact: There is no documentation impact.	2	25.2.200
38504941	EGW/IGW should include LCI header when the current load is less than or equals to the difference between previously reported load and configured LoadThreshold value	Egress Gateway and Ingress Gateway did not include the LCI header when the load-threshold condition was met. Doc Impact: There is no documentation impact.	3	25.2.102
38789763	IGW/EGW Pods are not coming up when localLciHeaderValidity is assigned with value 14400000, under lciheaderconfig	Ingress Gateway and Egress Gateway pods did not start when localLciHeaderValidity was set to 14400000. Doc Impact: There is no documentation impact.	3	25.2.106
38818360	ASM : helm install is failing with execution error at "custom-header.tpl:3:3): defaultVal is null" and same working fine in the 25.1.207 build	ASM Helm installation failed because custom-header.tpl received a null default value. Doc Impact: There is no documentation impact.	2	25.2.106
38460669	Requesting APIGW to provide a metric which give NFs the end to end latency	APIGW did not provide a metric for end-to-end NF latency. Doc Impact: There is no documentation impact.	Requesting APIGW to provide a metric which give NFs the end to end latency	25.2.101
38828770	/nf-common-component/v1/igw/applicationparams API is returning multiple entries during Policy NF upgrade causing pod resarts on audit service of PCF	The applicationparams API returned multiple entries during a Policy NF upgrade, causing audit-service pods to restart. Doc Impact: There is no documentation impact.	3	25.2.106

Table 4-14 (Cont.) Ingress Gateway 26.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38861854	Increase of failure rate % after in service upgrade to 24.2.4 and to 25.1.202	The traffic failure rate increased after in-service upgrades. Doc Impact: There is no documentation impact.	2	24.2.13
38992190	prioritymappingrules accepts invalid received range format without validation	prioritymappingrules accepted an invalid received-range format without validation. Doc Impact: There is no documentation impact.	3	26.1.200
38992126	prioritymappingrules allows leading-zero values for received/used, causing ambiguous/duplicate priority mappings	prioritymappingrules accepted leading-zero priority values, producing ambiguous or duplicate mappings. Doc Impact: There is no documentation impact.	4	26.1.200
38991946	prioritymappingrules validation rejects used as non-integer but rule-level detail is missing	prioritymappingrules rejected a non-integer used value without identifying the affected rule. Doc Impact: There is no documentation impact.	4	26.1.200
38992098	prioritymappingrules accepts duplicate received key within a rule object; last value silently overrides earlier value (last-key-wins)	prioritymappingrules accepted duplicate received keys within one rule and silently used the last value. Doc Impact: There is no documentation impact.	3	26.1.200
38992014	prioritymappingrules request with duplicate rules key is accepted; earlier rules array is silently overwritten (last-key-wins)	prioritymappingrules accepted duplicate rules keys and silently overwrote the earlier rules array. Doc Impact: There is no documentation impact.	3	26.1.200

Table 4-14 (Cont.) Ingress Gateway 26.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38991138	PUT global-configuration/ sbiserviceoperations behaves inconsistently with duplicate sbiServiceOperation keys (order-dependent)	The sbiserviceoperations PUT request handled duplicate sbiServiceOperation keys inconsistently based on their order. Doc Impact: There is no documentation impact.	3	26.1.200
38645273	Signature schemes in certificate request message TLS contains "not supported" values	TLS certificate-request messages included unsupported signature schemes. Doc Impact: There is no documentation impact.	3	25.1.200
38953545	jetty parameter MaxResponseHeaders Size" boundary check is missing	The non-ASM Jetty MaxResponseHeaders Size parameter did not have boundary validation. Doc Impact: There is no documentation impact.	3	26.1.200
39108214	IGW/EGW is not applying default rule while processing SMP Header request even when requestsmphheaders table in CCG is null.	Ingress Gateway and Egress Gateway did not apply the default rule to SMP-header requests when the requestsmphheaders table was null. Doc Impact: There is no documentation impact.	2	26.1.200
39009617	common_configuration _global table is getting updated even though applyHelmConfigOnUp grade is set to false with HELM upgrade.	A Helm upgrade updated common_configuration _global even when applyHelmConfigOnUp grade was false. Doc Impact: There is no documentation impact.	2	26.1.200
38943732	During upgrade and Rollback from 25.2.107 to 26.1.200-rc1 32% and 47%traffic loss observed.	Upgrade and rollback caused substantial traffic loss. Doc Impact: There is no documentation impact.	2	26.1.200

Table 4-14 (Cont.) Ingress Gateway 26.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
39028063	ASM:wrong error detail when helm upgraded with Pseudo range values in priority mapping rule configuration	An ASM Helm upgrade returned incorrect error details for pseudo-range priority-mapping values. Doc Impact: There is no documentation impact.	3	26.1.200
39005829	requestsmphheaders duplicate validation is case-sensitive	requestsmphheaders duplicate validation was case-sensitive. Doc Impact: There is no documentation impact.	4	26.1.200
39020622	No Input Validation on requestsmphheaders PUT Endpoint	The requestsmphheaders PUT endpoint did not validate input. Doc Impact: There is no documentation impact.	2	26.1.200
39033197	ASM:Error description for HELM upgrade failure and REST base upgrade failure should be in sync	Helm and REST-based upgrades returned inconsistent error descriptions for the same failure. Doc Impact: There is no documentation impact.	3	26.1.200
39031628	Not allowing sbiserviceoperations to be configured without initiatedRequestPriority Rule and responsePriorityRule key parameters using HELM install/upgrade	Helm installation and upgrade did not allow sbiserviceoperations to be configured without its priority-rule keys. Doc Impact: There is no documentation impact.	3	26.1.200
39046579	Outgoing message missing defaultSmpHeaderName name when incoming 3gpp-sbi-message-priority header value is out of range	Outgoing messages omitted defaultSmpHeaderName when the incoming message-priority value was out of range. Doc Impact: There is no documentation impact.	3	26.1.200

Table 4-14 (Cont.) Ingress Gateway 26.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
39155503	Wrong error message is sent in response when initiatedRequestPriorityRule or responsePriorityRule are empty or null	The response returned an incorrect error message when either priority rule was empty or null. Doc Impact: There is no documentation impact.	3	26.1.200
39154470	SBI Service Operations CNCC screen is not allowing to save modified entry	The SBI Service Operations CNC Console screen did not allow a modified entry to be saved. Doc Impact: There is no documentation impact.	3	26.1.200
38974389	To provide updated Grafana json wrt Spring Boot to 3.2.x upgrade changes for both IGW and EGW.	Grafana JSON was not updated for the Spring Boot 3.2.x changes. Doc Impact: There is no documentation impact.	3	26.1.200
39128713	no match route exception from egress gateway.	Egress Gateway returned a no-match-route exception. Doc Impact: There is no documentation impact.	2	26.1.200
38992215	prioritymappingrules inconsistent validation/ error messaging for defaultSmpHeaderName when empty string vs null	prioritymappingrules handled an empty defaultSmpHeaderName inconsistently with a null value. Doc Impact: There is no documentation impact.	4	26.1.200
38162347	for Custom Header request using REST-API, the complete array is not getting validated	REST API validation for custom-header requests did not validate the entire array. Doc Impact: There is no documentation impact.	3	25.1.203
36820640	Error Detail response for common config is not having Servicename and AppErrorCode in Error detail	Common Config error-detail responses omitted the service name and application error code. Doc Impact: There is no documentation impact.	3	24.2.4

Table 4-14 (Cont.) Ingress Gateway 26.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
35505051	Custom Package logging support for IGW & EGW	Ingress Gateway and Egress Gateway did not support custom-package logging. Doc Impact: There is no documentation impact.	3	23.2.0
38271114	Gateway configuration rollback does not work using FluxCD when it upgrades to a version it was deployed earlier	FluxCD could not roll back Gateway Services configuration to a version that had previously been deployed. Doc Impact: There is no documentation impact.	3	NA
37914904	Required Grafana dashboard JSON containing all the metrics for PI-B-25 PoP25 feature (IGW+EGW) along with Traffic success	The required Grafana dashboard JSON did not include all relevant metrics and traffic-success information. Doc Impact: There is no documentation impact.	4	25.1.200
34920448	NRF-Incorrect API gives 200 OK and creating config entry in DB for altRoute/logging	An invalid NRF API request returned HTTP 200 and created a configuration entry in the database. Doc Impact: There is no documentation impact.	4	22.2.0
38324716	Mounting of secrets is not backward compatible approach	Secret mounting was not backward compatible. Doc Impact: There is no documentation impact.	3	25.1.200
34609880	NFType dimension of oc_ingressgateway_htt p_requests_total is being set to incorrect value	The NFType dimension of the oc_ingressgateway_htt p_requests_total metric was set to incorrect value. Doc Impact: There is no documentation impact.	3	22.3.4

Table 4-14 (Cont.) Ingress Gateway 26.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36089938	errorcodeserieslist api allows configuration of errorCodeSeries having errorSet with no errorCodes	The errorcodeserieslist REST API allowed configuration of errorCodeSeries having errorSet with no errorCodes. Doc Impact: There is no documentation impact.	3	23.4.0
38411251	The Ingress gateway is sending 5xx responses while running Restfuzz on the NSSF microservices	The Ingress Gateway was sending 5xx responses while running Restfuzz on the NSSF microservices. Doc Impact: There is no documentation impact.	3	25.2.101
38284044	oc_oauth_request_failed_cert_expiry Metric not getting pegged	The oc_oauth_request_failed_cert_expiry metric was not recorded. Doc Impact: There is no documentation impact.	3	25.1.103
38148295	Some of the pod protection parameters validation happening with and without flag enabled. all parameters are not in sync.	Some of the pod protection parameters validation occurred with and without attribute enabled. All the parameters were not in synchronization. Doc Impact: There is no documentation impact.	4	25.1.200
38272205	fillrate accepting zero value and igw pod is restarting continuously when the pop feature is disabled	fillrate was accepting zero value and Ingress Gateway pod was restarting continuously when the Pod Protection using Rate Limiting feature was disabled. Doc Impact: There is no documentation impact.	3	25.1.200
35849764	Server header populated when nfiInstanceid not configured	The Server header populated when nfiInstanceid was not configured. Doc Impact: There is no documentation impact.	3	23.3.4

Table 4-14 (Cont.) Ingress Gateway 26.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38055583	all calls are failing when we configured routes via REST with pattern "pattern": "/npcf-smpolicycontrol/**/sm-policies"	All calls failed when routes were configured through REST APIs with pattern "pattern": "/npcf-smpolicycontrol/**/sm-policies". Doc Impact: There is no documentation impact.	3	25.1.201
35913266	In Policy Mapping Configuration in IGW, for the samplingPeriod parameter, validation of max value of parameter should be necessary	In Policy Mapping Configuration in Ingress Gateway, for the samplingPeriod parameter, validation of maximum value of the parameter was not mandatory. Doc Impact: There is no documentation impact.	4	23.3.0
34610831	IGW is accepting incorrect API names with out throwing any error	Ingress Gateway accepted incorrect API names without any error. Doc Impact: There is no documentation impact.	3	22.2.4
35913238	In IGW's Error Code Series Configuration, the names of the exceptionList and errorCodeSeries parameters are not verified.	In Ingress Gateway Error Code Series Configuration, the names of the exceptionList and errorCodeSeries parameters were not verified. Doc Impact: There is no documentation impact.	4	23.3.0
35932663	Key Validation is missing for IGW pod protection parameter name configuration	The Key validation was missing for the Ingress Gateway pod protection parameter name configuration. Doc Impact: There is no documentation impact.	3	23.3.3

Table 4-14 (Cont.) Ingress Gateway 26.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38159304	IGW is returning two different status codes in error response body when Configurable error code is true and non mandatory parameters are empty in errorCodeProfile.	Ingress Gateway returned two different status codes in error response body when Configurable error code was true and non mandatory parameters were empty in errorCodeProfile. Doc Impact: There is no documentation impact.	3	25.2.100
38470214	occnp_oc_ingressgateway_http_responses_total" metric not getting incremented	The occnp_oc_ingressgateway_http_responses_total metric did not get incremented. Doc Impact: There is no documentation impact.	3	24.2.7
38293029	High CPU utilisation was observed when OAuth feature is enabled with ASM	High CPU utilization was observed when OAuth feature was enabled with ASM. Doc Impact: There is no documentation impact.	3	25.2.100
38329632	Rename of the metric name - oc_ingressgateway_http_request_ratelimit_denied_count_total	The oc_ingressgateway_http_request_ratelimit_denied_count_total metric name was not renamed. Doc Impact: Renamed the oc_ingressgateway_http_request_ratelimit_denied_count_total metric to oc_ingressgateway_http_request_ratelimit_exceed_count_total in <i>Oracle Communications Cloud Native Core, Ingress Gateway User Guide</i> .	3	25.2.100

Table 4-14 (Cont.) Ingress Gateway 26.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
36604364	KeyId, certName, kSecretName, and certAlgorithm invalid values are not validating in the oauthvalidator configuration	KeyId, certName, kSecretName, and certAlgorithm invalid values were not validate in the oauthvalidator configuration. Doc Impact: There is no documentation impact.	3	24.1.0
35946896	Inconsistent behavior when Invalid Key vs Key not exist for mTLS	Inconsistent behavior when Invalid Key vs Key did not exist for mTLS. Doc Impact: There is no documentation impact.	4	23.3.4
36664352	KID is missing in access token, NSSF should send "Kid missing" instead of "kid configured does not match with the one present in the token"	If KID was missing in access token, NSSF should not have sent "Kid missing" instead of "kid configured does not match with the one present in the token". Doc Impact: There is no documentation impact.	3	24.1.6
38468707	IGW continues discarding discovery requests after overload trigger during ISSU, despite receiving normal load level signals	Ingress Gateway continued discarding discovery requests after overload was triggered during ISSU, despite receiving normal load level signals. Doc Impact: There is no documentation impact.	3	25.1.205
38369251	observed "Service MapDistCache has been terminated" in the old IGW pod after that new pods are not coming up when some of the IGW pods are deleted	Observed "Service MapDistCache has been terminated" in the old Ingress Gateway pod. After this, new pods failed to start when some Ingress Gateway pods were deleted. Doc Impact: There is no documentation impact.	3	25.2.100

Table 4-14 (Cont.) Ingress Gateway 26.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38339561	Metrics oc_ingressgateway_dd_unreachable and oc_egressgateway_dd_unreachable are not resetting to value zero after connection with DD is restored	The oc_ingressgateway_dd_unreachable and oc_egressgateway_dd_unreachable metrics were not resetting to value 0 after connection with Data Director was restored. Doc Impact: There is no documentation impact.	3	24.1.5
38593162	Request sent to IGW not getting forwarded to backend service	The request sent to Ingress Gateway was not forwarded to the back-end service. Doc Impact: There is no documentation impact.	2	25.2.200
37091738	HTTP/2 request dropped due to HTTP/1.1 validation	The HTTP/2 request dropped due to HTTP/1.1 validation. Doc Impact: There is no documentation impact.	3	23.1.0
38639858	Cnc-jetty : TLS- SETUP : IGW connections are increasing trend with kube-api-server when IGW installed freshly and Memory is increasing trend due to this connections.	Ingress Gateway connections to kube- api-server increased after a fresh Ingress Gateway installation, resulted in an increased memory. Doc Impact: There is no documentation impact.	2	25.2.200-rc.1
38867575	Metric oc_oauth_validation_fa ilure_total with invalid- scope dimension not pegged	The oc_oauth_validation_fa ilure_total metric with the invalid-scope dimension did not peg. Doc Impact: There is no documentation impact.	3	25.2.107

Table 4-14 (Cont.) Ingress Gateway 26.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38787849	New "tokenCacheSize" boundary value validation is not happening eventhough fresh install/upgrade is success.	New tokenCacheSize boundary value validation did not occur, even though the fresh installation or upgrade was successful. Doc Impact: There is no documentation impact.	3	25.2.106
38703469	allowedClockSkewSeconds IE value is wrongly configured in values.yaml file for IGW	allowedClockSkewSeconds IE value was incorrectly configured in the values.yaml file for Ingress Gateway. Doc Impact: There is no documentation impact.	2	25.2.200
38872538	IllegalArgumentException generated while recreating the new URI in Policy ipv6 setup causing all calls to fail with 500	IllegalArgumentExcepti on generated while recreating the new URI in Policy ipv6 setup causing all calls to fail with 500. Doc Impact: There is no documentation impact.	2	26.1.200
38767321	NPE and 500 internal ERROR observed in the POP25 error code rejections with configurable ERROR code.	NPE and 500 internal ERROR were observed in the Pod Protection using Rate Limiting error code rejections with configurable ERROR code. Doc Impact: There is no documentation impact.	2	25.2.106
38702154	After 1.5hrs run Continuous IRC are flooding in IGW when IGW freshly installed & Traffic loss is observed from 3K to 1.7K.	Continuous IRC was observed in Ingress Gateway when Ingress Gateway was freshly installed and traffic loss was observed from 3K to 1.7K. Doc Impact: There is no documentation impact.	1	25.1.207

Table 4-14 (Cont.) Ingress Gateway 26.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38808596	IGW failing the oauth token validation due to received token is not a digitally signed token instead NRF ID missing when validation mode is set to KID_PREFERRED	Ingress Gateway failed the OAuth token validation because the received token was not a digitally signed token instead NRF ID. Doc Impact: There is no documentation impact.	3	25.2.200
38569278	Ingress Gateway reports a NullPointerException after the installation of PCF	Ingress Gateway 25.2.200 reported NullPointerException after the installation of PCF. Doc Impact: There is no documentation impact.	3	25.2.200
38921131	When OC discards OverloadControlFilter attempts to update internal metrics using a null key or value, resulting in a NullPointerException in ConcurrentHashMap.put()	When Overload Control is discarded, OverloadControlFilter attempted to update internal metrics using a null key or value, resulted in a NullPointerException in ConcurrentHashMap.put(). Doc Impact: There is no documentation impact.	2	25.2.107
38462947	when 3gpp-Sbi-Correlation-Info is sent with empty value then it is also coming in response as empty when an error occurred at IGW	In Ingress Gateway 25.2.101, when 3gpp-Sbi-Correlation-Info was sent with empty value, it came in the response as empty when an error occurred at Ingress Gateway. Doc Impact: There is no documentation impact.	3	25.2.100
38908067	In IGW late arrival & Remove Header feature, call flow fail with the error as no matched http response found which was earlier running fine in 25.2.106 build	In Ingress Gateway late arrival and remove header feature, call flow failed with the error as no matched http response was found. Doc Impact: There is no documentation impact.	2	26.1.200

Table 4-14 (Cont.) Ingress Gateway 26.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38831358	Non-ASM: Memory leak observed in IGW Non-ASM set-up with 12k traffic, resulting IGW pod restarts after 7days of continuous run	A non-ASM memory leak was observed in an Ingress Gateway non-ASM setup with 12K traffic, resulting in an Ingress Gateway pod restart. Doc Impact: There is no documentation impact.	2	25.2.106
39064453	Label error_reason for metrics occnp_oc_ingressgateway_http_responses_total resulting in high Cardinality	Label error_reason for the occnp_oc_ingressgateway_http_responses_total metric resulted in high cardinality. Doc Impact: There is no documentation impact.	2	25.2.108
37079438	Routes Configuration under IGW is not raising an error when configured with an error code series id which is not already configured (when serverHeaderDetails param is enabled).	Routes Configuration under Ingress Gateway was not raising an error when configured with an error code series ID, which was not already configured when the serverHeaderDetails parameter was enabled. Doc Impact: There is no documentation impact.	4	24.3.1
38537413	convertHelmToRest is not merging routesconfiguration after upgrade for serverHeaderDetails	convertHelmToRest was not merging routesconfiguration after upgraded for serverHeaderDetails. Doc Impact: There is no documentation impact.	3	25.1.201

Table 4-14 (Cont.) Ingress Gateway 26.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
37046943	Mismatch in IGW occnp_oc_ingressgate way_http_requests_tot al & occnp_oc_ingressgate way_http_responses_t otal when request sent with Content-Length:0 and Body- PRESENT	Mismatch in Ingress Gateway occnp_oc_ingressgate way_http_requests_tot al and occnp_oc_ingressgate way_http_responses_t otal metrics was observed when the request was sent with Content-Length:0 and Body- PRESENT. Doc Impact: There is no documentation impact.	3	23.4.6
37986338	for XFCC header failure case "oc_ingressgateway_ht tp_responses_total" stats are not updated	For the XFCC header failure, the oc_ingressgateway_ht tp_responses_total metric was not updated. Doc Impact: There is no documentation impact.	4	25.1.200
38787543	With ratelimit feature , traffic rejections stats(oc_ingressgatew ay_http_responses_tot al) are not updated	With the rate limit feature, traffic rejections stats (oc_ingressgateway_ht tp_responses_total) were not updated. Doc Impact: There is no documentation impact.	3	25.2.106
37663139	For 404 not found "oc_ingressgateway_ht tp_requests_total" metrics are not updated only "oc_ingressgateway_ht tp_responses_tota" updated	For 404 not found, the oc_ingressgateway_ht tp_requests_total metric was not updated only oc_ingressgateway_ht tp_responses_tota was updated. Doc Impact: There is no documentation impact.	4	24.2.12

Table 4-14 (Cont.) Ingress Gateway 26.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38908204	In IGW Remove Header feature , IGW is not removing headers mentioned in removeRequestHeader and globalRemoveRequest Header while forwarding the request to backend servcie.	In the Ingress Gateway Remove Header feature, Ingress Gateway was not removing headers mentioned in removeRequestHeader and globalRemoveRequest Header while forwarding the request to the back-end service. Doc Impact: There is no documentation impact.	2	26.1.200
38879902	Misconfiguration + Pod Restart (multi fault scenario) leads to 100% traffic failure	Repeated Ingres Gateway pods restarted under load caused some pods to fail to load REST-mode route configurations, resulted in persistent 404 errors and an ingress traffic success rate drop by approximately 9%. Doc Impact: There is no documentation impact.	2	25.2.106
38691258	oc_oauth_keyid_count_total metric is not incrementing when validation mode is KID_PREFERRED/ KID_ONLY	The oc_oauth_keyid_count_total metric did not increment when validation mode was KID_PREFERRED/ KID_ONLY. Doc Impact: There is no documentation impact.	3	25.2.200

Table 4-14 (Cont.) Ingress Gateway 26.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
39151303	separate CIS/F5 labels for *-ingress-gateway-intra-nf service	In Gateway Services CNC Console 25.2.x, the *-ingress-gateway-intra-nf service inherited the main *-ingress-gateway service's F5 CIS labels, caused F5/CIS mapping conflicts and external FQDN routing issues in Webscale 1.3. Doc Impact: There is no documentation impact.	3	25.2.104
39112904	IGW is not adding SMP header to 2xx response when value of oc-backend-generated header is not exactly matched to the value adds-priority	Ingress Gateway was not adding SMP header to 2xx response when the value of oc-backend-generated header was not exactly matched to the value adds-priority. Doc Impact: There is no documentation impact.	2	26.1.200
38602425	Incorrect error response from IGW in case of an incorrect URI	Incorrect error response from Ingress Gateway was observed in case of an incorrect URI. Doc Impact: There is no documentation impact.	2	25.2.200
38611657	CNCC Ingress Gateway 500 â€œ reqHeaders null at CnccAuthorizationUtil.setRequestAttributes	The Spring Boot uplift caused Ingress Gateway to throw a null reqHeaders exception in CnccAuthorizationUtil.setRequestAttributes. Doc Impact: There is no documentation impact.	3	25.2.200

Table 4-14 (Cont.) Ingress Gateway 26.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38827897	cnc_jetty_service_disc overy metrics incorrectly pegged with value zero in ASM deployment	In ASM deployments, the cnc_jetty_service_disc overy metrics incorrectly remained at 0. Doc Impact: There is no documentation impact.	3	25.2.200

Note

Resolved bugs from 25.1.200 have been forward ported to Release 26.1.200.

4.2.11.3 Alternate Route Service Resolved Bugs

Release 26.1.201**Table 4-15 Alternate Route Service 26.1.201 Resolved Bugs**

Bug Number	Title	Description	Severity	Found in Release
38709256	Rollback fails due to Missing "empty-dir" volumeMount in 24.2.8-rc.3 ARS deployment.yaml (25.1.207)	Rollback failed because the earlier Alternate Route Service deployment.yaml file did not define the empty-dir volumeMount and volume required by the later deployment. Doc Impact There is no documentation impact.	3	25.1.207

Note

Resolved bugs from 25.1.200 have been forward ported to Release 26.1.200.

Release 26.1.200**Table 4-16 Alternate Route Service 26.1.200 Resolved Bugs**

Bug Number	Title	Description	Severity	Found in Release
38279138	NPE is seen Alternate route service during in- service upgrade from policy 25.1.200 to 25.2.100-rc1	NPE was observed alternate route service during in-service upgrade from Policy 25.1.200 to 25.2.100. Doc Impact: There is no documentation impact.	4	25.2.100

Table 4-16 (Cont.) Alternate Route Service 26.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38240183	NullPointerException in new ARS PODS when rollback to 25.1.203 from 25.2.100-rc2.	NullPointerException was observed in new Alternate Route Sservice pods during rollback to 25.1.203 from 25.2.100. Doc Impact: There is no documentation impact.	3	25.2.100
38594342	Alternate Route service reports a NullPointerException after the installation of PCF	25.2.200 Alternate Route Service reported a NullPointerException after the installation of PCF. Doc Impact: There is no documentation impact.	3	25.2.200
38831695	Different value getting configured for parameter "refresh-scheduler" in EGW and ARS microservice in comparison to what is present in values.yaml	Different values were getting configured for the parameter "refresh-scheduler" in Egress Gateway and Alternate Route Service microservice in comparison to what was present in values.yaml file. Doc Impact: There is no documentation impact.	3	25.2.106
38179432	During ARS Upgrade/Rollback from 24.2.13 to 24.2.15 Observed "IllegalStateException" on the 24.2.13 pods and No traffic drop observed	During Alternate Route Service upgrade and rollback from 24.2.13 to 24.2.15, "IllegalStateException" was observed on the 24.2.13 pods with no traffic drop. Doc Impact: There is no documentation impact.	3	24.2.15
38522842	First lookup call to ARS is failing for configured vFQDN	The initial Alternate Route Service lookup for a configured vFQDN failed, although subsequent lookups succeeded. Doc Impact: There is no documentation impact.	3	25.1.203
38405814	Post_rollback_SM_Validation fails at alternate-route logging level validation	After the rollback, system-manager validation failed while validating the Alternate Route Service logging level. Doc Impact: There is no documentation impact.	3	25.2.100
38997505	Unformatted WARN log "WARN found 2 argument placeholders, but provided 3 for pattern " is seen inpre-upgrade hook logs of alternate route, ingress-gw and egress-gw	The preupgrade hooks logged an unformatted WARN message because the placeholder count did not match the supplied arguments. Doc Impact: There is no documentation impact.	4	26.1.200

Table 4-16 (Cont.) Alternate Route Service 26.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38513360	IGW/EGW/ARS Deployment YAML having both "replicas" and "minReplicas/maxReplicas"	The deployment YAML file included both replicas and minReplicas/maxReplicas settings. Doc Impact: There is no documentation impact.	3	25.1.205
39060179	Upgrade to 26.1.2xx fails at nrf-client-nfdiscovery-pre-upgrade hook	The upgrade to Gateway Services 26.1.2xx failed in the nrf-client-nfdiscovery pre-upgrade hook. Doc Impact: There is no documentation impact.	2	25.2.200
38461465	Sender Attribute should only consist SEPP-<sepp-fqdn> when additional error logging is enabled in gw logging config	When additional error logging was enabled, the Gateway Services sender attribute was incorrectly populated. Doc Impact: There is no documentation impact.	4	25.2.100
39043146	Common-config-hook 26.1.200-rc.3 giving APPLICATION FAILED TO START error in app-info microservice hooks	The common-config hook caused the app-info microservice hooks to fail with an application-start error. Doc Impact: There is no documentation impact.	3	26.1.200
39061499	Common-Config: Alter Command not allowed	Common Config did not allow the required ALTER command. Doc Impact: There is no documentation impact.	2	26.1.200

Note

Resolved bugs from 25.1.200 have been forward ported to Release 26.1.200.

4.2.11.4 Common Configuration Service Resolved Bugs

Release 26.1.201

There are no resolved bugs in this release.

Release 26.1.200**Table 4-17 Common Configuration Service 26.1.200 Resolved Bugs**

Bug Number	Title	Description	Severity	Found in Release
38817454	IGW is unable to read the CCA secret when deployed with TLS v1.3	Ingress Gateway was unable to read the CCA secret when deployed with TLS v1.3. Doc Impact: There is no documentation impact.	2	25.2.106

Table 4-17 (Cont.) Common Configuration Service 26.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
38913633	Common-Config: GCC parameters should not be mandatory	The Global Common Config parameters were set as mandatory. Doc Impact: There is no documentation impact.	3	26.1.200
38099982	Common config rejection error detail should be proper - not like this Unexpected character ("\" (code 34)): was expecting comma to separate Object entries, Location :[Source: REDACTED (`StreamRead	Common Config rejection error details were incorrect because object entries were not separated by commas. Doc Impact: There is no documentation impact.	4	25.1.200

Note

Resolved bugs from 25.1.200 have been forward ported to Release 26.1.200.

4.2.11.5 NRF-Client Resolved Bugs

Release 26.1.204

There are no resolved bugs in this release.

Release 26.1.203

Table 4-18 NRF-Client 26.1.203 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
39663505	NRF Client emitted a stale ocLogId before updating the logging context	During NRF Discovery request processing, NRF Client emitted early request logs with an incorrect structured ocLogId. The incoming HTTP request contained the correct ocLogId header, but the JSON log field was populated from the previous request context before the logging context was updated. This resulted in incorrect request correlation during log analysis until the logging context was refreshed. Doc Impact: There is no documentation impact.	3	26.1.201

Table 4-18 (Cont.) NRF-Client 26.1.203 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
39316933	NRF Client NF Management failed while parsing text/plain responses from Config Server during scale down	During Config Server downtime, NRF Client NF Management received a text or plain response generated by the Envoy proxy instead of a JSON ProblemDetails response. NRF Client attempted to parse the response as ProblemDetails, resulting in a MessageBodyProviderNotFound Exception. This prevented NRF Client from gracefully handling non-JSON responses during Config Server scale down. Doc Impact: There is no documentation impact.	3	26.1.200
39253442	NRF Client NF Management INFO logs did not include ocLogId	NRF Client NF Management did not include the ocLogId field in INFO-level log messages. This reduced end-to-end request traceability and made log correlation more difficult during troubleshooting. Doc Impact: There is no documentation impact.	4	25.2.204

Release 26.1.202

There are no resolved bugs in this release.

Release 26.1.201

Table 4-19 NRF-Client 26.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
39350697	NRF Cache Auditor did not purge entries according to the configured percentage	The NRF Cache Auditor did not purge local cache entries according to the configured cleanup percentage because local cache cleanup was limited to the Discovery service. This resulted in stale cache entries remaining on the Management pod and prevented cache cleanup from operating according to the configured purge percentage. Doc Impact: There is no documentation impact.	2	25.2.200

Table 4-19 (Cont.) NRF-Client 26.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
39324695	NF Profile List API did not work as expected in CNC Console	The NF Profile List API did not function correctly in CNC Console. Saving populated configuration data failed with HTTP 400 Bad Request and the validation error CCS-E107, although the same configuration could be updated successfully by using the REST API. This prevented configuration updates through CNC Console while the REST API continued to function correctly. Doc Impact: There is no documentation impact.	2	26.1.200
39529740	NRF Client route-list notification to the Egress Gateway microservice was rejected as HTTP/1.x, preventing OAuth token retrieval	NRF Client sent route-list notifications to the Egress Gateway microservice by using HTTP/1.x, which the Egress Gateway microservice rejected. As a result, the dynamic NRF route list was not updated. This prevented successful OAuth token retrieval because the Egress Gateway microservice did not maintain the required dynamic NRF route information. Doc Impact: There is no documentation impact.	2	26.1.200
39251921	NRF Client NF Management did not handle non-JSON responses from Istio during ApplInfo Service scale down	During ApplInfo Service scale down, NRF Client NF Management received a plain-text HTTP 503 Service Unavailable response from the Istio Envoy proxy instead of a JSON ProblemDetails response. NRF Client attempted to parse the response as ProblemDetails. This resulted in exception processing instead of gracefully handling the non-JSON response. Doc Impact: There is no documentation impact.	3	26.1.200
39120111	NullPointerException occurred during heartbeat update processing when ipEndpoints was null	NRF Client generated a NullPointerException during heartbeat update post-response processing when the npcf-policyauthorization service contained ipEndpoints: null. This resulted in excessive exception logging and increased log volume during normal operation. Doc Impact: There is no documentation impact.	3	26.1.200

Table 4-19 (Cont.) NRF-Client 26.1.201 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
39232970	NRF NF Management generated repeated WARN logs for missing subscription renewal cache data	NRF NF Management generated the WARN log message Subscription renewal data does not exist in cache yet every 24 hours during normal operation. This resulted in repetitive WARN log entries that did not indicate an actual service issue. Doc Impact: There is no documentation impact.	3	26.1.200
39324939	NRF Route List API did not work as expected in CNC Console	The NRF Route List API did not function correctly in CNC Console. Saving populated configuration data failed with HTTP 400 Bad Request and the validation error CCS-E107, although the same configuration could be updated successfully by using the REST API. This prevented configuration updates through CNC Console while the REST API continued to function correctly. Doc Impact: There is no documentation impact.	3	26.1.200
39443980	Heartbeats were delayed to NRF, causing SEPP to enter the suspended state	In a non-ASM deployment, NRF Client Management did not support HTTP/2 communication with the Egress Gateway microservice after OAuth was disabled. The Egress Gateway microservice continued performing periodic health checks, but NRF Client Management communicated by using HTTP/1.1 instead of HTTP/2. This delayed heartbeat processing and caused SEPP to enter the suspended state. Doc Impact: There is no documentation impact.	3	25.1.200
39309686	ServiceDiscoveryException was observed in NRF pods after upgrade to 26.1.200	After an in-service upgrade from release 25.2.201 to 26.1.200, NRF pods continuously reported ServiceDiscoveryException errors during service discovery operations. This resulted in repeated service discovery failures after the upgrade and increased error logging. Doc Impact: There is no documentation impact.	3	26.1.200

Release 26.1.200

Table 4-20 NRF-Client 26.1.200 Resolved Bugs

Bug Number	Title	Description	Severity	Found in Release
39196633	PCF NRF-Client sent an invalid subscription request URI, causing subscription failure in NRF	NRF-Client sent an invalid URI in subscription requests initiated by PCF, causing NRF to reject the subscription request. NRF-Client also returned an incorrect error response structure when NRF notification delivery failed. This resulted in subscription failures and inconsistent error responses being returned for NRF notification failures. Doc Impact: There is no documentation impact.	3	25.2.202
39175786	NRF-Client Management Auditor Job emitted continuous WARN logs during normal cache audit	During normal NRF Client Management service operation, the scheduled auditor job generated WARN-level log messages every 30 minutes even though cache auditing completed successfully. This resulted in repetitive WARN log entries that increased log volume without indicating an actual service issue. Doc Impact: There is no documentation impact.	3	26.1.200

Note

Resolved bugs from 25.2.100 have been forward ported to Release 26.1.200.

4.3 Known Bug List

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

4.3.1 ATS Known Bugs

Release 26.1.201

There are no known bugs in this release.

4.3.2 CNC Console Known Bugs

Release 26.1.200

There are no known bugs in this release.

4.3.3 cnDBTier Known Bugs

Release 26.1.201

Table 4-21 cnDBTier 26.1.201 Known Bugs

Bug number	Title	Description	Customer impact	Severity	Found in release
3816619 1	Traffic failed after enabling Exception Table Cleanup-up feature	After enabling the feature, traffic failed during a PCF maintenance procedure because DBTier data pods restarted.	PCF loses nologging tables when DBTier data pods restart and interrupt maintenance. Workaround: Recover PCF and perform GRR to restore service with nologging-table data.	2	23.4.4
3826789 4	Ingress and egress traffic failed after rollback operation	Traffic failed after rollback when DBTier data pods restarted during PCF maintenance.	PCF loses nologging tables when DBTier data pods restart and interrupt maintenance. Workaround: Recover PCF and perform GRR to restore service with nologging-table data.	2	23.4.4
3842637 7	Management pods getting crashed	One of two mgmd pods disconnected; the other remained functional.	No impact to application database queries or georeplication. Workaround: During the next maintenance window, restart both mgmd pods simultaneously.	2	23.4.6
3841483 1	ndbmt-d-1 in CrashLoopBackOff	The ndbmt-d-1 data pod repeatedly restarted; its mate pod remained available.	No impact to application database queries or georeplication. Workaround: During the next maintenance window, scale down all data pods, then scale them up.	2	23.4.6

Table 4-21 (Cont.) cnDBTier 26.1.201 Known Bugs

Bug number	Title	Description	Customer impact	Severity	Found in release
39212897	Replication stopped with missing NDB\$BLOB record error	Replication stopped with a missing NDB\$BLOB_923_11 record error.	Replication breaks when this error occurs. Workaround: Back up the good site and perform GRR on the failed site.	2	25.2.102
39671872	GRR stuck in MONITOR_PARALLEL_BACKUP_RESTORE	Geo Replication Recovery (GRR) remained in MONITOR_PARALLEL_BACKUP_RESTORE for an extended period.	GRR does not progress beyond this state. Workaround: Restart the db-replication-svc pod.	2	26.1.200
39062625	GRR stuck when db-replication-svc PVC is deleted or wiped	Deleting or wiping the PVC during GRR can leave GRR stuck instead of transitioning to GRR_FAILED.	GRR remains stuck rather than entering the expected failed state. Workaround: Mark the site as failed with the REST API, then retry GRR.	3	25.2.201
39646621	hooks.sh --schema-upgrade SQL syntax error	Schema upgrade displays a SQL syntax error.	The upgrade may be reported as successful even when SQL queries fail. Workaround: Run the schema upgrade again.	3	26.1.200
39645167	dbtrecover stuck in INITIATE_PARALLEL_BACKUP_TRANSFER	dbtrecover gets stuck in INITIATE_PARALLEL_BACKUP_TRANSFER.	GRR does not progress beyond this state. Workaround: Increase MaxNoOfAttributes and perform a Helm upgrade.	3	26.1.200

Table 4-21 (Cont.) cnDBTier 26.1.201 Known Bugs

Bug number	Title	Description	Customer impact	Severity	Found in release
39357497	Exception entries and table mismatch after DBTier rollback	DBTier rollback can result in high exception-entry counts and mismatched table records.	Lost or skipped epoch transactions can cause database inconsistency when odd-indexed ndbmysqld pods are active replication channels. Workaround: Use --wait and --timeout during rollback: helm --namespace \$ {OCCNE_NAMESPACE} rollback \$CNDBTIER_RELEASE_NAME \$REVISION --wait --timeout 15m.	3	26.1.200
39616688	Replication break after deleting active mysqld pod with blank password encryption key	Deleting the active mysqld pod after setting a blank encryption key can break replication.	Invalid or blank password encryption keys can be accepted and cause issues. Workaround: Provide a valid key and use occndbtier_mksecrets_\${OCCNE_VERSION}.sh to create secrets.	3	26.1.200
39765309	Replication switchover can fail during maintenance activities	Restarting db-replication-svc during installation, upgrade, or rollback can prevent replication-channel details from loading.	Replication may fail and switchover may be unavailable. Check logs for Cannot invoke ... ReplicationSqlIp.getHostIp() . Workaround: Restart db-replication-svc pods at both sites.	3	26.1.201

4.3.4 CNE Known Bugs

Release 26.1.200

Table 4-22 CNE Release 26.1.200 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
36740199	BareMetal CNE installation on X9-2 servers fail	When installing OL9-based Bare Metal CNE on X9-2 servers, PXE booting may occur unexpectedly. Booting with the OL9.x ISO that uses the UEK kernel can hang with: Device does not have valid ME interface.	This issue prevents successful installation of Bare Metal CNE on X9-2 servers. Workaround: Use the hardware-agnostic CNE installation procedure for X9-2-based Bare Metal CNE deployments.	2	23.4.0
38106756	CNE self-upgrade failed due to Multus race condition	Intermittently, a CNE upgrade with CNLB enabled fails because Multus cannot remove required resources from a node.	This issue may occur during OCCNE upgrades with CNLB enabled. Workaround: Run the following command on all nodes: <code>sudo rm -R /opt/cni/bin/multus-shim</code> .	3	25.1.200
39722102	BareMetal deployment logs are incomplete on bastion	Expected complete pipeline and deployment logs should be saved on the bastion. However, <code>pipeline_bastion_*.log</code> stops midway at <code>initial_setup</code> .	Installation logs are not fully visible on the bastion host. Workaround: Run the pipeline command with <code>tee</code> . For example: <code>pipeline.sh tee pipeline_bastion_install.log</code> .	4	26.1.200

4.3.5 NSSF Known Bugs

Release 26.1.201

Table 4-23 NSSF 26.1.201 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37623199	Invalid Accept header can trigger an AMF notification and incorrect response for nssai-auth PUT and DELETE	NSSF does not consistently reject nssai-auth PUT and DELETE requests with an invalid Accept header. A PUT request can return HTTP 500 after storing data, and a DELETE request can return HTTP 204 without deleting data, which can trigger an AMF notification.	There is no impact on traffic or service behavior. Traffic processing and success rate remain unaffected. Workaround: There is no workaround.	3	25.1.100
37784755	Log-level change option is unavailable for ocnsf-ocpm-config and ocnsf-performance pods through CNCC and REST	The perf-info microservice does not provide an option to change the log level dynamically. Its log level is fixed at ERROR.	There is no impact on traffic or call processing because the perf-info microservice is not part of live traffic handling or the call-flow path. Production services remain unaffected. Workaround: There is no workaround.	3	25.1.100
38819395	NSSF nsselection pod restarts with exit code 143 during 80K TPS NS-Selection traffic when DB connectivity is cyclically interrupted	When DB connectivity to all pods is disrupted for 10 minutes and restored for 50 minutes, cyclically for more than 12 hours, one NS-Selection pod can restart with exit code 143.	Impact is low because the scenario is rare and environment-specific. Traffic resumes normally after the restart. During the restart window, only in-flight messages are affected, and only one of eight NS-Selection pods is impacted. Workaround: There is no workaround.	3	25.2.200

Table 4-23 (Cont.) NSSF 26.1.201 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
38621015	NSSF accepts overload threshold configuration when abatementValue is greater than onsetValue	NSSF accepts an overloadLevelThreshold configuration when abatementValue is greater than onsetValue. The configuration is saved, but the overload threshold is not applied, so overload behavior acts as if overload is disabled.	Misconfigured overload parameters can cause sustained overload control without proper recovery and lead to service degradation. Workaround: Configure overload-control parameters as documented in the Network Slice Selection Function REST Specification Guide. Set the abatement value lower than the onset value.	3	25.2.200
39660915	NSSF regression in 25.2.200: candidateAmfList format changed	The candidateAmfList format changes from an array of NfInstanceId strings to an array of objects containing nInstanceId.	AMF can report a decode error because it expects a string value in candidateAmfList but receives an object. Workaround: There is no workaround.	3	25.2.200

Table 4-23 (Cont.) NSSF 26.1.201 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
39604971	AutoConfig-Off: Duplicate element in ns-availability PATCH add request returns an error	In AutoConfig-Off mode, an ns-availability PATCH add request returns HTTP 400 INVALID_INPUT_DATA when it adds a duplicate TAI. The expected behavior is to accept the duplicate add request and retain one logical record.	Impact is low. There is no data loss or availability loss because the rejection indicates the original TAI already exists in NSSF. Workaround: Avoid sending duplicate TAI entries in PATCH add requests. If a duplicate request is rejected, send a PUT request with the complete intended NsAvailability content to synchronize the state.	3	26.1.200
39568412	Network Slice Selection Function User Guide counter mismatches	The User Guide contains metric and KPI documentation mismatches, including incorrectly formatted dimensions, inconsistent metric names or case, undocumented KPI metrics, and missing dimension information.	Using the guide for metric or KPI development, Prometheus dashboard creation, or query validation can result in incorrect metric names or labels, invalid queries, or confusion while validating NSSF counters. Workaround: Validate against Prometheus-visible metric names and labels until using a corrected version of the User Guide.	3	25.1.200

Table 4-23 (Cont.) NSSF 26.1.201 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
38973933	HTTP 500 and 404 responses in NS-Availability call flow after site restore	In a three-site GR deployment handling about 27K TPS per site, sequential failover and recovery of Sites 3 and 2 can result in isolated NS-Availability errors after traffic is redistributed.	Impact is minimal. Approximately 0.003% message loss is observed while two sites are down and traffic is handled by one active site. No prolonged outage occurs, and full replication and traffic distribution are restored after recovery. Workaround: There is no workaround.	4	25.2.200
39490419	NRF Client does not send unsubscribe messages for existing subscriptions when NSSF is uninstalled	When NSSF is uninstalled or deregistered from NRF in a GR deployment, NRF Client can fail to send unsubscribe requests for existing NRF subscriptions. Stale subscription records can remain in NfSubscriptions after the NSSF profile is removed.	Obsolete NSSF subscription state can remain in NRF, causing confusing database state, stale notification targets, repeated cleanup attempts, or extra triage during failover or uninstall validation. There is no loss of service. Workaround: Before uninstalling or scaling down, confirm that the NSSF nfInstanceId in NRF Client configuration matches the profile registered in NRF. After uninstall or deregistration, check NfSubscriptions for stale records and remove them using the NRF subscription delete API or a supported NRF cleanup procedure.	4	26.1.200

Table 4-23 (Cont.) NSSF 26.1.201 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
38628736	NSSF pods enter Error state before termination when all deployments are scaled down to zero	During scale-down of all NSSF deployments to zero replicas, several pods briefly enter the Error state before terminating.	There is no impact on live traffic because this occurs during intentional scale-down to zero. The issue is limited to pod lifecycle behavior during shutdown. Workaround: There is no workaround.	4	25.2.200

4.3.6 OCCM Known Bugs

Release 26.1.200

There are no known bugs in this release.

4.3.7 OSO Known Bugs

Release 26.1.200

Table 4-24 OSO Known Bugs 26.1.200

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
38661250	IPv6 connections are not established between prom-svr and NF pods when OSO is deployed in IPv6-preferred mode.	Prometheus targets, pods, endpoints, and services use IPv4 addresses even when the cluster is dual-stack.	Targets use IPv4 even in a dual-stack cluster. There is no functional impact because OSO supports PreferredDualStack mode, which permits IPv4 fallback. Workaround: There is no workaround.	3	25.2.200

Table 4-24 (Cont.) OSO Known Bugs 26.1.200

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
39143113	Communication between OSO-PROM, OSO-ALM, and OSO-APM uses IPv4 addresses instead of IPv6.	In a dual-stack cluster, communication from ALM to the APM service uses IPv4 addresses.	OSO component communication uses IPv4 even in a dual-stack cluster. There is no functional impact because OSO supports PreferredDualStack mode, which permits IPv4 fallback. Workaround: There is no workaround.	3	25.2.200

4.3.8 NRF Known Bugs

Release 26.1.201

Table 4-25 NRF 26.1.201 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
39690026	NRF request combinations changed from 5xx responses to other HTTP status codes	NRF returns different HTTP status codes for some request combinations than in previous releases. Certain request combinations return HTTP 503 Service Unavailable instead of HTTP 500 Internal Server Error while continuing to report an error condition.	The response code changes from HTTP 500 Internal Server Error to HTTP 503 Service Unavailable, which can affect applications that explicitly depend on the previous status code while handling error responses. Workaround: There is no workaround.	3	25.2.201

Table 4-25 (Cont.) NRF 26.1.201 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
39690007	NRF request combinations changed from 4xx responses to other HTTP status codes	NRF returns different HTTP status codes for some request combinations than in previous releases. Certain request combinations return a different HTTP 4xx response code while continuing to report the same client error condition.	The HTTP response code for certain 4xxerror conditions changes, which can affect applications that rely on specific 4xxstatus codes for error handling. Workaround: There is no workaround.	3	25.2.201
39588761	NRF does not consistently preserve the existing Via header chain when forwarding subscription update and delete requests	NRF does not consistently preserve the existing Via header chain when forwarding subscription update and delete requests. Instead of appending the local Via entry, NRF drops the existing Via header chain before forwarding the request.	Dropping earlier Via header values makes subscription update and delete forwarding behavior inconsistent with discovery, Access Token, profile retrieval, subscription create, and roaming forwarding flows. Because the Via header is used for forwarding hop history and loop detection, dropping earlier entries reduces loop detection visibility across multiple NRF hops. Workaround: There is no workaround.	3	26.1.200

Table 4-25 (Cont.) NRF 26.1.201 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
39273759	NRF Nnrf_NFManagement_NfUpdate accepts add / nfStatus for an existing attribute and emits an inconsistent NF_PROFILE_CHANGED partial notification	NRF accepts Nnrf_NFManagement_NfUpdate request that uses the add operation for an existing nfStatus attribute and updates the NF status. The generated NF_PROFILE_CHANGED partial notification contains op=ADD with the original value instead of the expected op=REPLACE.	NRF updates the nfStatus successfully but sends subscribers an inconsistent NF_PROFILE_CHANGED notification. Applications that process partial notifications based on the operation type can observe incorrect notification semantics. Workaround: There is no workaround.	3	26.1.200

4.3.9 SCP Known Bugs

Release 26.1.201

Table 4-26 SCP 26.1.201 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
38952387	Case mismatch in Localities for INTER SCP cases (USWEST and USWest) results in incorrect population of worker inter-SCP routing maps	A case mismatch in localities for inter-SCP scenarios, such as USWEST and USWest, results in incorrect population of worker inter-SCP routing maps.	Inter-SCP routing is affected only when localities are misconfigured. Workaround: Correct locality information in the NF profile.	3	25.2.200

Table 4-26 (Cont.) SCP 26.1.201 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
38782868	Routing continues to a deleted NF type when profile deregistration fails	Routing continues to a deleted NF type when profile deregistration fails.	Routing can continue using stale rules when an NF type is deleted but its profile deregistration fails. This has very low functional impact because of the limited use case. Workaround: Do not delete the NF type configuration while NF profiles are still registered.	3	25.2.200
38008367	Overlapping regex validation missing for apiSpecificResourceUri in routing configuration API	The routing configuration REST API allows overlapping regex patterns in the apiSpecificResourceUri field, leading to ambiguous routing when a request matches multiple patterns.	Conflicting routing-configuration selection can occur when regex patterns overlap in apiSpecificResourceUri. Workaround: Do not configure overlapping regex patterns.	3	25.1.100
37995299	SCP cannot delete foreign SCP routing details after deregistration	When a foreign SCP profile is unregistered, SCP fails to remove associated routing details for certain profiles.	There is no impact because SCP redeployment is required to update nfsetid, and that is not a recommended change. Workaround: There is no workaround.	3	25.1.200
37970295	Worker pod restart observed due to coherence timeout when a single cache pod is used	When increasing the number of worker pods from 1 to 23 with only one cache pod, worker pods restart because of a coherence timeout.	A deployment with a single cache pod can result in worker-pod restarts under high rate-limit traffic. Workaround: There is no workaround.	3	25.1.200

Table 4-26 (Cont.) SCP 26.1.201 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
37949191	ocscp_metric_nf_lci_tx_total increments when no LCI headers are received from peer NFs	The ocscp_metric_nf_lci_tx_total metric increments even when no LCI headers are received from peer NFs.	There is a minor observability impact. Workaround: There is no workaround.	3	25.1.200
37622431	Audit failures observed during overload when traffic exceeds pod limits by 50%	When traffic operates at maximum rated capacity and exceeds pod limits by 50%, audit failures occur while SCP is in overload condition.	In overload conditions, the SCP Worker pod-protection mechanism discards some internally generated NRF audit requests. Workaround: Audits are periodic and eventually succeed after the overload condition subsides.	3	25.1.100
37575057	Duplicate routing when producer responses contain a Location header in 3xx cases	SCP performs duplicate routing when the producer NF responds with a Location header in 3xx cases.	SCP sends requests to the producer NF again when the producer NF in the redirect URL and alternate routing rules are the same. Workaround: There is no workaround.	3	25.1.100
36757321	429 errors due to pod-overload discards during upgrade and rollback	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 429 errors.	Some traffic loss can occur during an upgrade under bursty traffic conditions because of the SCP Worker pod-protection mechanism. Workaround: Perform upgrades during periods of low traffic to avoid overloading pods.	3	24.2.0

Table 4-26 (Cont.) SCP 26.1.201 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
39740833	Intermittent duplicate on-demand audits during static-to-DNS NRF migration	During static-to-DNS NRF migration, SCP can queue two on-demand audits when DNS SRV targets for the same NRF set are created sequentially and the preferred NRF changes during evaluation.	On-demand audit requests can be duplicated in some cases, but there is no functional impact. Workaround: There is no workaround.	3	26.1.201
39732803	interPlmnFqdnValidationEnabled deploys as false although documentation states the default is true	SCP deploys interPlmnFqdnValidationEnabled as false, while documentation identifies the default value as true.	For fresh installations, the default value should be true. If it is not set, SCP alternate routing does not restrict routing to inter-PLMN FQDNs. Workaround: Use the System Options REST API to explicitly set interPlmnFqdnValidationEnabled to true.	3	25.1.205
39715345	Notification-rejection metric is not updated under queue-full conditions with multiple updates for the same NF	SCP does not increment ocsdp_notification_nf_profile_rejected_total when a full notification queue receives multiple updates for the same NF.	If a persistently high rate of NF profile notifications is sent to SCP over an extended period, the metric is not incremented. This can affect observability by preventing accurate metric reporting. Workaround: Monitor queue-full metrics and notification logs to identify and investigate these conditions.	3	26.1.200

Table 4-26 (Cont.) SCP 26.1.201 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
39690644	Model-D discovery cache is not updated by local refresh after producer NF status-change notification in inter-SCP routing	For inter-SCP routing, SCP does not update the Model-D discovery cache through local refresh after receiving a producer NF status-change notification.	There is no functional impact on Model-D-based routing when the Model-D cache is enabled. NF status changes are applied during NRF_REFRESH instead of LOCAL_REFRESH. Workaround: There is no workaround.	3	26.1.200
39678455	Outlier Detection PUT API does not apply defaults for omitted optional fields before persistence or SSE	The Outlier Detection PUT API does not apply default values for omitted optional attributes before persisting and applying the configuration.	If optional attributes are omitted from the REST API request payload, default values are not applied and the Outlier Detection configuration can behave incorrectly. Workaround: After configuring an Outlier Detection rule, verify that all relevant attributes are present. Explicitly include all attributes defined in the payload, including optional ones.	3	26.1.200
39672610	Runtime-update ATS lacks a case where an error profile is configured with 3xx error codes	ATS does not cover the runtime-update case in which an error profile specifies 3xx error codes.	There is no functional impact. Manual testing confirmed that the functionality works as expected. Workaround: There is no workaround.	3	26.1.200

Table 4-26 (Cont.) SCP 26.1.201 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
39672032	SCP NRF Bootstrap Info Migration performs audit for non-applicable NRF sets in migrated mode	In migrated mode, SCP can initiate an on-demand audit for NRF sets that do not apply when the performAudit attribute changes from false to true.	There is no functional impact. Changing performAudit from false to true for an NRF set triggers on-demand audits for non-applicable NRF sets whose attribute is already true. Workaround: There is no workaround.	3	25.2.104
39671406	scp51 retains Outlier Detection state from the previous scenario after profile deregistration	SCP can retain the previous Outlier Detection state for an inter-SCP destination after the foreign SCP NF profile is deregistered.	In a rare condition, the prior Outlier Detection state is not cleared after the foreign SCP NF profile is deregistered. This issue could not be reproduced. Workaround: Ensure that either a successful response is received or no traffic is sent to this peer SCP destination during the interval configured in the Outlier Detection rule.	3	26.1.200

Table 4-26 (Cont.) SCP 26.1.201 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
39588774	SCP does not return redirect response with alternate URI	In an inter-SCP routing scenario, SCP cannot reselect and route a request when a producer-side SCP returns a self-generated 307 redirect response with an alternate SCP URI.	If the producer-side SCP returns a self-generated 307 Redirect response containing the redirect URL of another producer-side SCP, the consumer-side SCP cannot reselect the redirected SCP and route to it. Workaround: Do not return a 307 Redirect response containing a redirect URL in this scenario.	3	26.1.200
39587422	Inconsistent ocscp_peer_scp_fqdn values are reported in peer-SCP unhealthy metrics	The ocscp_peer_scp_fqdn dimension can report an IP address instead of an FQDN in peer-SCP unhealthy metrics.	There is no functional impact. The dimension can display an IP address regardless of whether host preference is configured to use an FQDN or IP address. Workaround: There is no workaround.	3	26.1.200
39525762	Error cause and detail need an update during deletion of a 3GPP-defined discovery query parameter	Documentation specifies an incorrect error cause and detail for deletion of a 3GPP-defined discovery query parameter.	There is no functional impact. Workaround: There is no workaround.	3	26.1.200
39523758	CNLB annotation examples are missing from SCP documentation	SCP documentation does not include CNLB annotation examples.	There is no functional impact. Workaround: There is no workaround.	3	25.1.204

Table 4-26 (Cont.) SCP 26.1.201 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
39505209	NF profiles learned through a deleted NRF Set ID are not deregistered	When an NRF Set ID is removed from the NRF bootstrap configuration, SCP does not automatically deregister NF profiles learned through that NRF Set.	When an NRF set is configured and the network topology is learned through it, removing the NRF set from the NRF bootstrap configuration does not automatically remove the related learned topology. Workaround: Remove the NRF set only after all NFs registered through it have been deregistered. Alternatively, use a script, such as one using <code>curl</code> , to explicitly deregister associated NF profiles before removing the NRF set.	3	26.1.200
39491413	Unable to configure Consumer Info Configuration	SCP returns an insufficiently specific REST API configuration error when it cannot configure Consumer Info Configuration.	There is no functional impact. The REST API error message needs to provide a more specific reason for the error. Workaround: There is no workaround.	3	26.1.200
39417928	scpinstanceid and operation="NF_LIST_RETRIEVAL" are missing from the ocscp_audit_tx_req_total user-guide entry	The SCP user guide does not document scpinstanceid and operation="NF_LIST_RETRIEVAL" for ocscp_audit_tx_req_total.	There is no functional impact. Workaround: There is no workaround.	3	26.1.200

Table 4-26 (Cont.) SCP 26.1.201 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
39348771	Range of priority, capacity, and load for the self SCP profile is missing from the User Guide and REST Guide	The SCP User Guide and REST API Guides do not document the ranges for priority, capacity, and load in the self SCP profile.	There is no functional impact. Workaround: There is no workaround.	3	26.1.200
39332752	SCP inquiry about recommended tolerationSeconds values for NoExecute toleration	The documented behavior for tolerationSeconds does not state the recommended value for a NoExecute toleration when an SCP pod is evicted and rescheduled.	There is no functional impact. This scenario evaluates the time required to evict and reschedule an SCP pod after a Kubernetes node becomes unreachable or enters the NotReady state. The current default is 300 seconds. Workaround: Set tolerationSeconds to 0 for immediate eviction. Configure this value through annotations.	3	25.1.200
39332708	Error cause and detail are incorrect for an invalid baseEjectionTime value in Outlier Detection configuration	SCP returns an incorrect error cause and detail for an invalid baseEjectionTime value in Outlier Detection configuration.	There is no functional impact. The level of detail in error messages for mandatory or optional attributes with out-of-range values is under review. Workaround: There is no workaround.	3	26.1.200
39304820	SCP profile configuration update and deletion need correction in the CNCC section of the User Guide	The CNC Console section of the SCP User Guide does not describe SCP profile configuration updates and deletion.	There is no functional impact. Workaround: There is no workaround.	3	26.1.200

Table 4-26 (Cont.) SCP 26.1.201 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
39270613	Canary Release feature details	Canary configuration changes can continue to use Model-D cached data, and single-digit capacity values can produce weights that do not achieve the intended traffic distribution.	Changes to the canary attribute or canary traffic percentage might not take effect for Model-D-based traffic because routing continues to use cached data. Single-digit capacity values can also produce weights too low to achieve the intended traffic-distribution ratio. Workaround: Disable the Model-D cache before applying canary configuration changes through the REST API, then re-enable it afterward. Configure capacity values in the canary NF profile as multiples of 100.	3	24.3.0
39189619	SCP intermittently returns 504 TARGET_NOT_REACHABLE for AMF notifications after successful AMF profile retrieval	SCP intermittently returns 504 TARGET_NOT_REACHABLE for an AMF notification after successfully retrieving the AMF profile from NRF.	There is no functional impact because multiple NF profiles cannot have the same FQDN within the network. Workaround: There is no workaround.	3	25.2.200
38098107	SCP does not consider Version and Trailer fields from Jetty response	SCP does not consider version and trailer fields from Jetty responses.	There is no impact because these fields are not currently used. Workaround: There is no workaround.	4	25.1.200

Table 4-26 (Cont.) SCP 26.1.201 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
38079614	SCP All Services: Replace <code>java.util.Date</code> and <code>org.joda.time</code> with <code>java.time</code>	SCP services rely on <code>java.util.Date</code> and <code>org.joda.time</code> for date and time handling, which are not thread-safe and lack modern functionality.	There is no impact because this is a minor code enhancement. Workaround: There is no workaround.	4	25.1.200
39715249	SCP logs "Exception occurred. Failed to get ServiceEntry" while deregistering an NF profile	SCP logs the exception when it deregisters an NF profile that has no services.	There is no functional impact. The log message is misleading because no service entry is expected for an NF profile without services. Workaround: There is no workaround. The log message can be safely ignored.	4	26.1.200
39710459	Low-severity code issues identified during the 26.1.200 release code audit	Low-severity code issues identified during the SCP 26.1.200 code audit remain open.	There is no functional impact. Multiple issues identified during the code-review audit are addressed. Workaround: There is no workaround.	4	26.1.200
39664694	"Page not found" exceptions occur in the configuration pod during a Model-D duration run	During a Model-D duration run, the configuration pod logs "Page not found" exceptions for non-SBI requests that use an incorrect resource URI.	There is no functional impact. Some non-SBI requests, such as metrics-scraping requests, use an incorrect resource URI and cause this error. Workaround: Correct the resource path, or safely ignore the error if it is expected.	4	26.1.200

Table 4-26 (Cont.) SCP 26.1.201 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
39458013	SMF ingress NF type reconfiguration does not update fallback ingress_SMF-NA bucket	Reconfiguring the SMF ingress NF type does not update the fallback ingress_SMF-NA bucket, leaving a stale rate-limit value.	Customer impact was not provided. Workaround: There is no workaround.	4	26.1.200
39418028	Pod name is reported twice in ocscp_worker_health_check_rx_req_total	The ocscp_worker_health_check_rx_req_total metric reports the pod-name dimension twice.	There is no functional impact. The pod-name dimension appears twice only for this metric. Workaround: There is no workaround.	4	26.1.200
39148745	Global error handler maps validation and deserialization errors to INVALID_VALUE instead of 3GPP-compliant causes	The global error handler maps validation and deserialization errors to INVALID_VALUE rather than applicable 3GPP causes such as MANDATORY_IE_INCORRECT and OPTIONAL_IE_INCORRECT.	There is no functional impact. The traffic feed-related configuration APIs must be aligned with 3GPP specifications. Workaround: There is no workaround.	4	26.1.200

4.3.10 SEPP Known Bugs

Release 26.1.200

Table 4-27 SEPP 26.1.201 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
39138384	SEPP does not remove x-next-hop-authority header for requests toward Remote PLMN	SEPP forwards x-next-hop-authority and other x-headers to the partner. Removing these headers globally breaks N32-C routing. The issue requires header handling for N32-F and N32-C traffic.	There is a security breach risk during RH SEPP to E// SEPP integration. Workaround: There is no workaround.	3	25.1.201

Table 4-27 (Cont.) SEPP 26.1.201 Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
39131855	Conformance HTTP/2: Request with nonconforming pseudo-headers is not considered malformed	SEPP handles malformed HTTP/2 pseudo-header requests incorrectly. A request missing :scheme returns 404, and a request missing :method gives no response instead of a stream reset or protocol error.	Standards conformance affects interoperability and testing. Workaround: There is no workaround.	3	25.1.201
39091133	Intermittent failures observed in multiple Create and Delete RS and RSS call flows - v25.2.200	In 25.2.200-rc.1, CreateRSS, CreateRS, DeleteRSS, and DeleteRS flows intermittently return 500, 403, or 404 instead of the expected 201 or 204 responses. This indicates inconsistent behavior in RS and RSS operations.	RS and RSS lifecycle call flows have internal stability and reliability impact. Workaround: There is no workaround.	3	25.2.200
39332895	SEPP: Inquiry about recommended tolerationSeconds values for NoExecute toleration	SEPP requires guidance for recommended NoExecute toleration values so that pods can be evacuated after node shutdowns or reboots.	Customers need guidance for SEPP pod evacuation behavior after abrupt shutdowns or reboots. Workaround: No final workaround is documented; internal portfolio/SA review is pending.	3	25.1.200
39559658	Default error code profile mentioned in "Pod Protection by Rate Limiting" does not exist	The default error-code profile referenced under Pod Protection by Rate Limiting does not match the profile available in Error Code Profiles.	Default error-code profile references are inconsistent between Pod Protection by Rate Limiting and Error Code Profiles. Workaround: No explicit workaround is documented in Jira.	3	26.1.200

SEPP 26.1.200 Gateway Known Bugs

Table 4-28 SEPP 26.1.200 Gateway Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
38810446	[SEPP-APIGW] Missing ignoremaxresponse time & sbiRoutingWeightBasedEnabled under metadata in EGW CNCC screen	The Egress Gateway CNC Console screen does not show ignoremaxresponse time and sbiRoutingWeightBasedEnabled under metadata. Because the SBITimer feature behavior depends on these metadata values, users cannot include them when they configure or edit routes through CNC Console.	SBITimer and NRF route automation functionality over Egress Gateway are impacted, and the feature may not work correctly. Workaround: Configure through Helm.	3	26.1.200
38810483	[SEPP-APIGW] No support for header based predicate under EGW Routesconfiguration in CNCC screen	The Egress Gateway Routes configuration screen in CNC Console does not support header-based predicates.	Users are impacted when they configure routes through REST with a header name as the filter. Workaround: Configure through Helm.	3	26.1.200
38769835	[SEPP-IGW] SBITimer Feature: Misleading logger in the IGW, when request contains 3gpp-Sbi-Origination-Timestamp and gpp-Sbi-Sender-Timestamp but no 3gpp-Sbi-Max-Rsp-Time	IGW prints a misleading log message when the request includes 3gpp-Sbi-Origination-Timestamp and 3gpp-Sbi-Sender-Timestamp but does not include 3gpp-Sbi-Max-Rsp-Time. The log suggests that sender or origin headers are missing instead of indicating that 3gpp-Sbi-Max-Rsp-Time is missing.	Users may be misled when they review the logs. Workaround: There is no workaround.	3	26.1.200
38771574	[SEPP-IGW] SBITimer Feature Enabled-sbiTimerTimezone related Issues	The sbiTimerTimezone behavior has multiple issues. When the gateway is configured as ANY and the request contains PDT timezone, processing uses GMT instead of PDT. When the gateway is configured as ANY and the request has no timezone, a Late Arrival Error occurs. When the gateway is configured as GMT and the request contains PDT, the expected behavior is unclear.	Not provided. Workaround: Not provided.	3	26.1.200

4.3.11 Common Services Known Bugs

4.3.11.1 Alternate Route Service Known Bugs

Release 26.1.2xx

There are no known bugs in this release.

4.3.11.2 Egress Gateway Known Bugs

Release 26.1.2xx

Table 4-29 Egress Gateway 26.1.2xx Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
39123626	DestinationHost dimension is missing from the outgoing IP type metric	The DestinationHost dimension is absent from the occnp_oc_egressgateway_outgoing_ip_type metric in Gateway Services 25.2.109.	Observability in error scenarios and system performance are affected. Workaround: There is no workaround.	3	25.2.109
38304085	EGW does not validate 3gpp-sbi-message-priority parameters during POP25 and overload	Egress Gateway does not validate the 3gpp-sbi-message-priority header parameters in pod-protection overload scenarios.	Invalid values can cause the feature to malfunction. Workaround: The consumer NF should send valid header values.	3	25.2.100
39088228	Host dimension in Egress Gateway response metrics still has cardinality explosion	The Host dimension remains part of the response-metric cardinality in the Egress Gateway 25.2.109 test release.	Observability in error scenarios and system performance are affected. Workaround: There is no workaround.	3	25.2.109
39049678	Improve logging for NPE during Jetty bean creation when TLS is disabled	An unexpected NullPointerException error log can be emitted during REST API mode installation while Jetty web-client beans are created with TLS disabled.	Installation observability may be affected by the unexpected error log. Workaround: There is no workaround.	3	25.2.108

Table 4-29 (Cont.) Egress Gateway 26.1.2xx Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
38810483	No support for header-based predicates in EGW route configuration on the CNCC screen	The CNCC screen does not support configuring a header-based predicate for Egress Gateway routes.	NRF route configuration can be affected because it relies on a header-based predicate at PLMN Egress Gateway, potentially affecting inter-PLMN NRF requests through SEPP. Workaround: There is no workaround.	3	25.2.106
38294514	NPE during OAuth access request when nrfClientQueryEnabled is enabled	A NullPointerException occurs during an OAuth access request when nrfClientQueryEnabled is enabled.	The OAuth token request does not reach NRF, causing additional calls to fail. Workaround: There is no workaround.	3	25.2.100
38279961	oauthDeltaExpiryTime functionality does not work during traffic	Egress Gateway can request an NRF OAuth token before the configured oauthDeltaExpiryTime has expired.	No traffic impact because token processing occurs before timer expiry. Workaround: There is no workaround.	3	25.2.100
38778598	Outgoing IP type metric remains IPv4 after DNS changes to IPv6	In an IPv6-preferred dual-stack deployment, the outgoing IP type metric can remain set to IPv4 after DNS removes the IPv4 address.	The metric can report incorrect active-connection information after DNS address-family changes. Workaround: There is no workaround.	3	25.2.104
38810446	Required metadata parameters are missing from the EGW CNCC screen	The CNCC screen does not expose ignoremaxresponstertime and sbiRoutingWeightBasedEnabled under Egress Gateway route metadata.	Producer-NF load sharing is unavailable by default, and SBITimer cannot be used for PLMN Egress Gateway unless IgnoreMaxRspTimeHeader is explicitly configured. Workaround: Configure the routes using REST APIs instead of using the CNC Console.	3	25.2.106

Table 4-29 (Cont.) Egress Gateway 26.1.2xx Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
38351114	EGW returns 500 instead of 503 when a configured static NRF is unavailable	When a static NRF is unavailable, Egress Gateway returns an HTTP 500 internal-server error instead of the expected HTTP 503 service-unavailable response.	The response does not clearly identify the static NRF availability failure. Workaround: There is no workaround.	4	25.2.100
39016184	TLS connection and disconnection logs are missing in Egress Gateway	Egress Gateway does not produce messages confirming successful TLS connection establishment or disconnection. Corresponding messages remain available in Ingress Gateway.	Not provided. Workaround: There is no workaround.	4	26.1.200

4.3.11.3 Ingress Gateway Known Bugs

Release 26.1.2xx

Table 4-30 Ingress Gateway 26.1.2xx Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
38405814	Post-rollback validation fails at alternate-route logging-level validation	After rollback, SM validation reports a mismatch in the Alternate Route logging-level values.	No production impact. The log level is not changed from WARN to DEBUG. Workaround: There is no workaround.	3	25.2.100
39706472	Failure counts are updated for services regardless of whether ocPolicyMapping is enabled	Failure counts can be maintained for route-configured services absent from ocPolicyMapping. PerfInfo and APIGW use only OC-policy-mapped services for overload calculation and action.	No functional impact to NRF. Workaround: There is no workaround.	3	26.1.204
38310333	IGW request and response latency metrics are not updated for TLS 401 rejection	In a TLS setup, Ingress Gateway request and response latency metrics are not updated when Ingress Gateway rejects a request with HTTP 401.	Observability is affected because the latency metric is not updated. Workaround: There is no workaround.	3	25.2.100

Table 4-30 (Cont.) Ingress Gateway 26.1.2xx Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
35526243	Operational state change should be disallowed when required pre-configurations are absent	Ingress Gateway allows an operational-state change even when <code>controlledshutdownerrormapping</code> and <code>errorcodeprofiles</code> are not configured. A pre-check should prevent the state change when these required configurations are missing.	Gateway Services may process a request that should have been rejected. Workaround: There is no workaround.	3	23.2.0
38902043	Configurable error-code profiles incorrectly include "Name or service not known" in <code>error_reason</code>	Ingress Gateway appends "Name or service not known" to the configured <code>error_reason</code> value for all error-code profiles. The error reason should contain only the configured value.	No traffic impact. Workaround: There is no workaround.	4	26.1.200
38807819	Incorrect OAuth error response when producer PLMN ID validation fails	Ingress Gateway can reject an OAuth token with a 401 response even when the token contains the correct producer PLMN ID. The returned title also incorrectly refers to an NRF instance-ID mismatch.	A valid request can be rejected with an incorrect OAuth validation response. Workaround: There is no workaround.	3	25.2.200
38293511	IGW does not validate <code>3gpp-sbi-message-priority</code> parameters during POP25 and overload	Ingress Gateway does not validate the <code>3gpp-sbi-message-priority</code> header parameters in pod-protection overload scenarios.	Invalid values can cause the feature to malfunction. Workaround: The consumer NF should send valid header values.	3	25.2.100
39706361	Overload failure count is not aligned for all IGW-generated 4xx and 5xx error codes	Ingress Gateway-generated validation failures occur before the request reaches the backend and are therefore not counted for backend overload control. Configured failure counting applies to matching backend responses and supported Ingress Gateway-to-backend exceptions.	No functional impact to NRF or backend overload handling. Workaround: There is no workaround.	3	26.1.204
38769987	SBITimer time-zone mismatch gauge does not reset	The <code>oc_ingressgateway_sbitimer_timezone_mismatch</code> metric remains at 1 after it is pegged and does not reset to 0.	Observability is affected because the metric does not reset. Workaround: There is no workaround.	3	25.2.105

Table 4-30 (Cont.) Ingress Gateway 26.1.2xx Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
39527997	Intermittent NullPointerException in IGW when a route has an empty CustomReqHeaderEntryFilter headers list	When an Ingress Gateway route is configured through REST with an empty CustomReqHeaderEntryFilter headersList, an intermittent NullPointerException can occur while processing traffic, resulting in an HTTP 500 response.	Not provided. Workaround: There is no workaround.	3	26.2.200
38771574	SBITimer time-zone handling issues	When the configured time zone is ANY or GMT, certain timestamp and missing-time-zone combinations can be interpreted incorrectly and return an incorrect late-arrival error.	Requests can receive an incorrect late-arrival error instead of the expected format or time-zone handling. Workaround: Ensure that the configuration and timestamp header use compatible time zones.	3	25.2.105

4.3.11.4 Common Configuration Service Known Bugs

Release 26.1.2xx

Table 4-31 Common Configuration Service 26.1.2xx Known Bugs

Bug Number	Title	Description	Customer Impact	Severity	Found in Release
39063477	Missing upper-limit validation allows oversized global configuration objects	Global Configuration APIs do not enforce maximum item counts. Oversized configurations can be persisted and may fail later or affect runtime processing.	Potential performance, memory, database, or processing impact when oversized configurations are loaded and evaluated. Workaround: There is no workaround.	3	26.1.200

4.3.11.5 NRF-Client Known Bugs

Release 26.1.2xx

There are no known bugs in this release.