Oracle® Communications
Cloud Native Core Release Notes

Release 2.4.0

F46564-11

October 2021

Oracle Communications Cloud Native Core Release Notes, Release 2.4.0

F46564-11

Contents

1 Introduction

2 Feature Descriptions

3 Media and Documentation

4 Resolved and Known Bugs

My Oracle Support

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

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

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

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

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

What's New In This Guide

This section introduces the documentation updates for Release 2.4.0 in Oracle Communications Cloud Native Core (CNC) Release Notes.

Release 2.4.0 - F46564-11, October 2021

cnDBTier Release 1.9.2

The following sections are updated for cnDBTier Release 1.9.2:

- Media Pack: Added Media pack details
- CNE Resolved Bugs: Added cnDBTier resolved bugs list

Release 2.4.0 - F46564-10, October 2021

SEPP Release 1.6.1

SEPP Resolved Bugs: Modified the description of resolved bug.

Release 2.4.0 - F46564-09, October 2021

SEPP Release 1.6.1

The following sections are updated for SEPP Release 1.6.1:

- Media Pack: Added Media pack details
- Common Services Load Lineup: Added Common Services Load Lineup details
- SEPP Resolved Bugs: Added resolved bugs list
- SEPP Customer Known Bugs: Added customer known bugs list
- Security Compliance Information: Added Security Compliance Information

Release 2.4.0 - F46564-08, October 2021

SCP Release 1.14.1

The following sections are updated for SCP Release 1.14.1:

- Media Pack: Added Media pack details
- SCP Resolved Bugs: Added resolved bugs list

NRF Release 1.14.1

The following sections are updated for NRF Release 1.14.1:

- Network Repository Function (NRF): Added new features or enhancements
- Media Pack: Added Media pack details
- Common Services Load Lineup: Added Common Services Load Lineup details
- NRF Resolved Bugs: Added resolved bugs list

Release 2.4.0 - F46564-07, October 2021

CNC Console Release 1.8.1

The following sections are updated for CNC Console Release 1.8.1:

- Cloud Native Core Console (CNC Console): Added new features/enhancements
- Media Pack: Added Media pack details
- Security Compliance Information: Added Security Compliance Information
- CNC Console Resolved Bugs: Added resolved bugs list

Release 2.4.0 - F46564-06, October 2021

CNC Policy Release 1.14.1

The following sections are updated for CNC Policy Release 1.14.1:

- Cloud Native Core Policy (CNC Policy): Added new features or enhancements
- Media Pack: Added Media pack details
- Common Services Load Lineup: Added Common Services Load Lineup details
- CNC Policy Resolved Bugs: Added resolved bugs list

BSF Release 1.10.1

The following sections are updated for BSF Release 1.10.1:

- Binding Support Function (BSF): Added new features or enhancements
- Media Pack: Added Media pack details
- Common Services Load Lineup: Added Common Services Load Lineup details
- BSF Resolved Bugs: Added resolved bugs list

Release 2.4.0 - F46564-05, October 2021

CNE Release 1.9.1

The following sections are updated for CNE Release 1.9.1:

- Cloud Native Environment (CNE): Updated the features information
- Media Pack: Added Media pack details
- CNE Resolved Bugs: Added resolved bugs list

Release 2.4.0 - F46564-04, September 2021

CNE Release 1.9.0

The following sections are updated for CNE Release 1.9.0:

- Cloud Native Environment (CNE): Added new features/enhancements
- Media Pack: Added Media pack details
- CNE Resolved Bugs: Added resolved bugs list
- CNE Customer Known Bugs: Added customer known bugs list

Release 2.4.0 - F46564-03, August 2021

CNC Policy Release 1.14.0

The following sections are updated for CNC Policy Release 1.14.0:

- Cloud Native Core Policy (CNC Policy): Added new features/enhancements
- Media Pack: Added Media pack details
- Common Services Load Lineup: Added Common Services Load Lineup details
- CNC Policy Resolved Bugs: Added resolved bugs list
- CNC Policy Customer Known Bugs: Added customer known bug list

BSF Release 1.10.0

The following sections are updated for BSF Release 1.10.0:

- Binding Support Function (BSF): Added new features/enhancements
- Media Pack: Added Media pack details
- Common Services Load Lineup: Added Common Services Load Lineup details
- BSF Resolved Bugs: Added resolved bugs list
- BSF Customer Known Bugs: Added customer known bug list

NSSF Release 1.7.0

NSSF Customer Known Bugs: Removed the customer known bugs list

Release 2.4.0 - F46564-02, August 2021

SCP Release 1.14.0

The following sections are updated for SCP Release 1.14.0:

- Service Communication Proxy (SCP): Added new features or enhancements
- Media Pack: Added Media pack details
- Security Compliance Information: Added Security Compliance Information
- SCP Resolved Bugs: Added resolved bugs list

Release 2.4.0 - F46564-01, August 2021

CNC Console Release 1.8.0

The following sections are updated for CNC Console Release 1.8.0:

- Cloud Native Core Console (CNC Console): Added new features/enhancements
- Media Pack: Added Media pack details
- Security Compliance Information: Added Security Compliance Information
- CNC Console Resolved Bugs: Added resolved bugs list

SEPP Release 1.6.0

The following sections are updated for SEPP Release 1.6.0:

- Security Edge Protection Proxy (SEPP): Added new features or enhancements
- Media Pack: Added Media pack details
- Common Services Load Lineup: Added Common Services Load Lineup details
- SEPP Resolved Bugs: Added resolved bugs list
- Security Compliance Information: Added Security Compliance Information

NRF Release 1.14.0

The following sections are updated for NRF Release 1.14.0:

- Network Repository Function (NRF): Added new features or enhancements
- Media Pack: Added Media pack details
- Security Compliance Information: Added Security Compliance Information
- NRF Resolved Bugs: Added resolved bugs list
- NRF Customer Known Bugs: Added customer known bugs list

NSSF Release 1.7.0

The following sections are updated for NSSF Release 1.7.0:

- Network Slice Selection Function (NSSF): Added new features or enhancements
- Media Pack: Added Media pack details
- Common Services Load Lineup section.
- Security Compliance Information: Added Security Compliance Information
- NSSF Resolved Bugs: Added resolved bugs list
- NSSF Customer Known Bugs: Added customer known bugs list

UDR Release 1.14.0

The following sections are updated for UDR Release 1.14.0:

- Unified Data Repository (UDR): Added new features or enhancements
- Media Pack: Added Media pack details
- Security Compliance Information: Added Security Compliance Information
- UDR Resolved Bugs: Added resolved bugs list
- UDR Customer Known Bugs: Added customer known bugs list

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 2.4.0.

Binding Support Function (BSF)

BSF 1.10.1 has been updated with the following enhancement:

- **Compatibility with OCCNE 1.9.1**
  BSF is compatible with OCCNE 1.9.1. For more information about OCCNE 1.9.1, see *Oracle Communications Cloud Native Environment Installation Guide*.

Binding Support Function (BSF) 1.10.0 is updated with the following enhancements:

- **Diameter Gateway Pod Congestion Control:** BSF is enhanced with a congestion control mechanism for Diameter Gateway at pod level. With this new feature, configurations can be done through CNC Console or REST API to determine the congestion state of a pod and trigger congestion control. For more information, see "Diameter Gateway Pod Congestion Control" in *Oracle Communications Cloud Native Core Binding Support Function User Guide*.
- **SBI Error Codes:** BSF is designed to handle Protocol, Application, and a few other additional defined errors for different scenarios. When BSF encounters error in processing a request, it sends error codes in the response message to the request. With this enhanced functionality, BSF allows users to configure error codes by adding customized values, for a defined condition, for the following fields:
  - Error Description
  - HTTP Status Code
  - Application Error Code

  For more information, see "SBI Error Codes" in *Oracle Communications Cloud Native Core Binding Support Function User Guide*.
- **Bulk Export:** BSF is enhanced to support bulk export of BSF Managed Objects (MOs) and their dependencies using CNC Console. For more information on the enhancements on CNC Console for this feature, see "Configuring BSF using CNC Console" in *Oracle Communications Cloud Native Core Binding Support Function User Guide*.

Cloud Native Core Console (CNC Console)

Cloud Native Core Console (CNC Console) 1.8.1 has been updated with the following enhancement:

- **CNE 1.9.0 Metrics and Alerts Support:** CNC Console Metrics, CNC Console KPIs, and CNC Console Alerts are updated to support CNE 1.9.0. For more information, see CNC Console Metrics, CNC Console KPIs, and CNC Console Alerts sections in *Oracle Communications Cloud Native Core Console User Guide*.

- **CNCC IAM Keycloak Upgraded from 10.0.2 to 15.0.2:** The CNCC IAM Keycloak version is upgraded from 10.0.2 to 15.0.2. For more information, see Setting up CNC Console IAM section in *Oracle Communications Cloud Native Core Console User Guide*.

Cloud Native Core Console (CNC Console) 1.8.0 has been updated with the following enhancements:

- **CNC Console Multi–Cluster deployment support:** In multi-cluster deployment, a single CNC Console can manage NF instances that access different Kubernetes clusters. The multi-cluster deployment provides the selection of the particular cluster at the top level of the CNC Console GUI. For more information, see *Oracle Communications Cloud Native Core Console Installation and Upgrade Guide* and *Oracle Communications Cloud Native Core Console User Guide*.

  SEPP-CNC Console Integration: SEPP is integrated with CNC Console. The integration allows users to configure SEPP using the CNC Console. For more information, see *Oracle Communications Cloud Native Core Console User Guide.*

Cloud Native Diameter Routing Agent (CnDRA)

There are no new features or updates implemented in CNC 2.4.0 release.

Cloud Native Environment (CNE)

Oracle Communications Cloud Native Environment (OC-CNE) 1.9.0 has been updated with the following enhancements:

- **HA Load Balancing for vCNE:** Redundant load balancers are now deployed for each external network, working as an active or standby pair. When the active load balancer fails, CNE detects the failure and automatically activate the standby load balancer. For more information, see *Oracle Communications Cloud Native EnvironmentInstallation Guide* and *Oracle Communications Cloud Native Environment Upgrade Guide*.
- **HA Prometheus:** OC-CNE supports the deployment of redundant Prometheus instances. Each Prometheus collects metrics from all 5G NFs and OC-CNE common services. This redundant data collection prevents against gaps in metrics data if one of the redundant Prometheus instances fails, and during maintenance operations. For more information, see *Oracle Communications Cloud Native Environment Installation Guide* and *Oracle Communications Cloud Native Environment Upgrade Guide*.
- **Customer PKI Integration with Platform Service Mesh:** The OCCNE platform service mesh can now use certificates from the customer's certificate authority (CA) when generating X.509 certificates for use in mTLS. The Intermediate CA issuer, where the customer generates a certificate at their CA and delivers it to OC-CNE for use as an intermediate CA, is the only supported issuer type in this release. For more information, see *Oracle Communications Cloud Native Environment Installation Guide* and *Oracle Communications Cloud Native Environment Upgrade Guide*.
- **Support for DB Tier 4-Site Replication:** The cnDBTier is enhanced to support replication of the data stored in DB Tier to as many as 3 additional sites. Hence, it supports 4-Site, 3-Site, and 2-Site replication to ensure better service availability. For more information, see *Oracle Communications Cloud Native Core DBTier User's Guide*.

- **DBTier support for Non-georeplication SQL Nodes:** The cnDBTier supports a separate statefulset of non-georeplication SQL nodes that is not part of georeplication configuration. The cnDBTier consists of two set of SQL nodes one which is configured for georeplication and the other to handle application traffic. The applications that utilize the MySQL connectivity service to connect to the MySQL NDB cluster will be using the non georeplication SQL nodes.
- **DBTier supports MySQL version 8.0.24:** The cnDBTier supports Oracle MySQL Cluster Database version 8.0.24.

CNC NF Data Collector

There are no new features or updates implemented in CNC 2.4.0 release.

Cloud Native Core Policy (CNC Policy)

CNC Policy 1.14.1

CNC Policy 1.14.1 has been updated with the following enhancement:

- **Compatibility with OCCNE 1.9.1**
  CNC Policy is compatible with OCCNE 1.9.1. For more information about OCCNE 1.9.1, see *Oracle Communications Cloud Native Environment Installation Guide*.

CNC Policy 1.14.0

Oracle Communications Cloud Native Core Policy (CNC Policy) 1.14.0 has been updated with the following enhancements:

- **Support for 3GPP NF Sets and Binding Headers:** CNC Policy supports the 3GPP NF Sets and Binding Headers in Direct and Indirect communication. For more information, see "Support for 3GPP NF Sets and Binding Headers" in *Oracle Communications Cloud Native Core Policy User Guide*.
- **Four-Site Georedundancy:** CNC Policy is enhanced to support the four-site Geographical Redundant (Georedundant) deployment. It offers, four-site, three-site, and two-site georedundancy to ensure service availability when one of the Policy sites is down. For more information, see "Georedundancy Support" in *Oracle Communications Cloud Native Core Policy User Guide*.
- **Diameter Gateway Pod Congestion Control:** CNC Policy is enhanced with a congestion control mechanism for Diameter Gateway at pod level. With this new feature, configurations can be done through CNC Console or REST API to determine the congestion state of a pod and trigger congestion control. For more information, see "Diameter Gateway Pod Congestion Control" in *Oracle Communications Cloud Native Core Policy User Guide*.
- **Topology Hiding for Diameter Gateway:** CNC Policy provides support for topology hiding for diameter gateway. For more information, see "Topology Hiding for Diameter Gateway" in *Oracle Communications Cloud Native Core Policy User Guide*.
- **Enhancements in Policy Conditions and Actions**: The Policy conditions and actions have been updated in PCRF project. For more information, see *Oracle Communications Cloud Native Core Policy Design Guide*.

Inter-Working Function (IWF)

There are no new features or updates implemented in CNC 2.4.0 release.

Service Communication Proxy (SCP)

SCP 1.14.0 has been updated with the following enhancements:

- **Multiple SCP Deployment in the Same Kubernetes Cluster**
  This feature allows you to deploy multiple SCP instances in the same Kubernetes cluster. Each SCP instance is deployed in a different namespace and is independent of each other. These SCP instances can use the same cnDBTier with a unique database name or a dedicated cnDBTier during the installation. For more information about this feature, see *Oracle Communications Cloud Native Core Service Communication Proxy User Guide*.
- **Support for SCP Triplet Deployment**
  Using the Triplet Deployment model, you can configure three SCP instances as mates for georedundancy. Each SCP instance in a triplet is configured to manage the overall traffic expected for the triplet so that when two SCP instances are unavailable, the single SCP instance can manage the overall traffic. For more information about this feature, see *Oracle Communications Cloud Native Core Service Communication Proxy User Guide*.
- **Support for SCP Upgrade and Rollback**
  SCP can be upgraded to a new version and rolled back to a previous supported version as described in *Oracle Communications Cloud Native Core Service Communication Proxy Installation and Upgrade Guide*.
- **Support for Disaster Recovery**
  SCP deployment and database can be recovered using the disaster recovery tasks. For more information, see *Oracle Communications Cloud Native Core Service Communication Proxy Disaster Recovery Guide*.
- **Support for scp-worker Large Profile**
  SCP supports the scp-worker service configuration with large profile. For more information, see the "Resource Requirements" in *Oracle Communications Cloud Native Core Service Communication Proxy Installation and Upgrade Guide*.
- **Multipart Message Support**
  The multipart message support is enable in SCP. For more information, see 3GPP Specifications.

Security Edge Protection Proxy (SEPP)

Security Edge Protection Proxy (SEPP) 1.6.x has been updated with the following enhancements:

- **Automated Test Suite (ATS) Integration and Enhancement**:
  SEPP provides Automated Test Suite for validating the functionalities. Jenkins plugin of Test Result Analyzer is also added. For more information about ATS integration, see *Oracle Communications Cloud Native Core Automated Test Suite Guide*.
- **CNC Console GUI Integration**:

SEPP is integrated with CNC Console. This allows the user to configure SEPP Rest APIs using the CNC Console GUI. For more information about SEPP integration, see *Oracle Communications Cloud Native Core Security Edge Protection Proxy User Guide.*

Network Exposure Function (NEF)

There are no new features or updates implemented in CNC 2.4.0 release.

Network Repository Function (NRF)

OCNRF 1.14.1 has been updated with the following enhancement:

- **OCNRF Compatibility with OCCNE 1.9**
  OCNRF is compatible with OCCNE 1.9.0. For more information about OCCNE 1.9.0, see *Oracle Communications Cloud Native Environment Installation Guide*.
- **OCNRF Disaster Recovery Guide**
  *Oracle Communications Cloud Native Core Network Repository Function Disaster Recovery Guide*is delivered in NRF documentation package. The Disaster Recovery Guide describes scenario based procedures used to perform disaster recovery of Oracle Communications Network Repository Function (OCNRF) deployments. The OCNRF operators can take database's backup and restore them either on same or a different cluster. It uses OCNRF database for commands or instructions.

OCNRF 1.14.0 has been updated with the following enhancement:

- **NRF Roaming Support**
  This feature is to support the 3GPP defined inter-PLMN routing for NRF specific service operations like NFDiscover, AccessToken, NFStatusSubscribe, NFStatusUnSubscribe, and NFStatusNotify. For more information about roaming feature, see the "Roaming Support" chapter in *Oracle Communications Cloud Native Core Network Repository Function User Guide*.
- **NRF Forwarding Decision Per NF Type and NF Service Type**
  OCNRF Forwarding feature is enhanced to enable the users to define more controlled forwarding criteria for NFDiscover and AccessToken Service Requests from OCNRF to an intermediate NRF. The user can configure the preferred NF Type, the NF Services, or both for which forwarding is applicable. This provides the flexibility to regulate the traffic between the NRFs. For more information about forwarding feature, see the "OCNRF Forwarding" chapter in *Oracle Communications Cloud Native Core Network Repository Function User Guide*.
- **Support for R16 Parameters as per 29.510**
  Support for smfInfoList and smfInfo attribute as per 29.510-g70 for NFRegister, NFUpdate, NFStatusSubscribe, NfStatusNotify and NfDiscover.
- **Failure KPIs per Service Operation**
  Added new failure KPIs to measure the requests and responses per service operations For more information about KPIs, see *Oracle Communications Cloud Native Core Network Repository Function User Guide*.

Network Slice Selection Function (NSSF)

OCNSSF 1.7.0 has been updated with the following enhancements:

- **Feature Negotiation**: OCNSSF now supports feature negotiation mechanism that is used to negotiate the optional features applicable between the NSSF and the NF Service

Consumer, for the NSSF supported services. The following optional features have been added under the Feature Negotiation feature:

For more information about the applicable helm parameters, see *Oracle Communications Cloud Native Core Network Slice Selection Function Installation and Upgrade Guide.*

For more information, see *Oracle Communications Cloud Native Core Network Slice Selection Function User's Guide*.

- **Subscription Modification (SUBMOD)**: It's an optional feature under the Feature Negotiation feature that allows operators to modify subscriptions by supporting HTTP Patch on NsAvailability Subscription. To enable the SUBMOD feature, it is mandatory to enable the Feature Negotiation feature.
  For more information about the applicable helm parameters, see *Oracle Communications Cloud Native Core Network Slice Selection Function Installation and Upgrade Guide*.

  For more information on the feature description, see *Oracle Communications Cloud Native Core Network Slice Selection Function User's Guide.*

- **Empty Authorized NSSAI Availability Notification (EANAN)**: It's an optional feature that provides support for sending an empty array of Authorized NSSAI Availability Data when a notification trigger leads to a situation of no Tracking Area (TA) with Authorized NSSAI by the NSSF. To enable the EANAN feature, it is mandatory to enable the Feature Negotiation feature.
  For more information about the applicable helm parameters, see *Oracle Communications Cloud Native Core Network Slice Selection Function Installation and Upgrade Guide*.

  For more information on the feature description, see *Oracle Communications Cloud Native Core Network Slice Selection Function User's Guide.*

Unified Data Management (UDM)

There are no new features or updates implemented in CNC 2.4.0 release.

Unified Data Repository (UDR)

UDR 1.14.0 has been updated with the following enhancements:

- **Overload Control:** UDR supports overload management as it helps to control services downtime and ensures service availability during extreme overload conditions. It uses Ingress Gateway and perf-info microservices to control network congestion and handles the overload scenarios. For more information about this feature, see *Oracle Communications Cloud Native Core Unified Data Repository User Guide*.

- **Export and Import of UDR Configuration Data:** With the implementation of export and import feature, UDR enable its users to perform bulk export and import of UDR configuration data using CNC Console. For more information about this feature, see the "Export & Import" section in *Oracle Communications Cloud Native Core Unified Data Repository User Guide*.

- **iXML to CSV converter for bulk import:** With the introduction of CSV conversion tool, UDR enable its users to convert subscriber records in iXML format to CSV format. The iXML format is same as defined for 4G UDR. For more information, see the "Bulk Import Tool" section in *Oracle Communications Cloud Native Core Unified Data Repository User Guide*.

- **Diameter Gateway for UDR Sh interface:** UDR provides a way to handle overload of backend microservices for different thresholds and types of overload scenarios. For more information, see the "Architecture" and "Metrics" sections in *Oracle Communications Cloud Native Core Unified Data Repository Users Guide* and "Configurable Parameters" section in *Oracle Communications Cloud Native Core Unified Data Repository Installation and Upgrade Guide*.
- **Integration with common NRF Client:** UDR integration with NRF client project provides support for NFSetID and Locality configuration in NFProfile of UDR.

  For more information about NRF Client integration, see the "Configuring Unified Data Repository" section in *Oracle Communications Cloud Native Core Unified Data Repository Installation and Upgrade Guide*.
- **Support for Database Backup and Recovery:** UDR provides feature to enable its users to perform database backup and recovery under different scenarios like configuration database corrupted, configuration and subscribers database corrupted, single site failure etc. For information about how to overcome the identified disaster recovery scenarios, see *Oracle Communications Cloud Native Core Unified Data Repository Disaster Recovery Guide*.
- **Service Mesh Charts:** UDR supports virtual service and Request Authentication CRDs in the Helm charts. For more information, see *Oracle Communications Cloud Native Core Unified Data Repository Installation and Upgrade Guide*.
- **Support of UDR MIBs:** UDR provides MIB files for UDR alerts, which can be integrated with SNMP.
- **OAM Interface for Provisioning Gateway:** UDR-ProvGw now provides an OAM interface using which configurations of Ingress Gateway, Egress Gateway, and Provisioning Gateway services can be configured using REST APIs. For more information, see *Oracle Communications Cloud Native Core Provisioning Gateway Interface Specification Guide*.

3 Media and Documentation

Media Pack

This section lists the media package for Cloud Native Core 2.4.0. To download the media package, refer to MOS.

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

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

Table 3-1 Media Pack Contents for Cloud Native Core 2.4.0

Description	Versions	ATS Test Cases Included	Upgrade	Compliance
Oracle Communications Cloud Native Core Binding Support Function (BSF)	1.10.1	Yes **Note:** Not applicable to: • Support for Debug Tool • Consistent Logging Level Support	Supports fresh installation as well as upgrade from 1.9.x to 1.10.1.	Compatible with: • NRF 1.14.0 • UDR 1.14.0 • Policy 1.14.1 • cnDBTier 1.9.1 • OSO 1.7.0 • ASM 1.6.14-am4 • CNE 1.9.1
Oracle Communications Cloud Native Core Binding Support Function (BSF)	1.10.0	Yes **Note:** Not applicable to: • Support for Debug Tool • Consistent Logging Level Support	Supports fresh installation as well as upgrade from 1.9.x to 1.10.0	Compatible with: • NRF 1.14.0 • UDR 1.14.0 • Policy 1.14.0 • CNDBTier 1.8.7 • OSO 1.7.0 • ASM 1.6.14-am4 • CNE 1.8.3

Table 3-1 (Cont.) Media Pack Contents for Cloud Native Core 2.4.0

Description	Versions	ATS Test Cases Included	Upgrade	Compliance
Oracle Communications Cloud Native Core Console (CNC Console)	1.8.1	NA	Supports fresh installation as well as upgrade from CNC Console 1.7.x, 1.8.0 to 1.8.x	Compatible with: • SCP 1.14.0 • NRF 1.14.1 • UDR 1.14.0 • Policy 1.14.1 • BSF 1.10.0 • SEPP 1.6.0 • CNDBTier 1.8.x,1.9.1 • OSO 1.6.2 • Kubernetes 1.18.8 • ASM 1.5.7-am3 / 1.4.6-am9 / 1.6.14-am4 • CNE 1.7.x,1.8.x, 1.9.1 (CNC Console Multi-Cluster deployment requires OCCNE 1.9.x to enable OCCNE Common Services)

Table 3-1 (Cont.) Media Pack Contents for Cloud Native Core 2.4.0

Description	Versions	ATS Test Cases Included	Upgrade	Compliance
Oracle Communications Cloud Native Core Console (CNC Console)	1.8.0	NA	Supports fresh installation as well as upgrade from CNC Console 1.7.x to 1.8.0	Compatible with: • SCP 1.14.0 • NRF 1.14.0 • UDR 1.14.0 • Policy 1.14.0 • BSF 1.10.0 • SEPP 1.6.0 • CNDBTier 1.8.x,1.9.0 • OSO 1.6.2 • Kubernetes 1.18.8 • ASM 1.5.7-am3 / 1.4.6-am9 / 1.6.14-am4 • CNE 1.7.x,1.8.x, 1.9.0 (CNC Console Multi-Cluster deployment requires OCCNE 1.9.x to enable OCCNE Common Services)
Oracle Communications Cloud Native Core Diameter Routing Agent (CnDRA)	1.6.0	NA	Supports fresh installation only	NA
Oracle Communications Cloud Native Core DBTier	1.9.2	NA	cnDBTier 1.9.2 supports fresh installation. The upgrade from cnDBTier 1.8.x to 1.9.x is supported.	NA
Oracle Communications Cloud Native Core Cloud Native Environment (CNE)	1.9.1	NA	CNE 1.9.1 supports fresh installation. The upgrade from CNE 1.8.4 to 1.9.1 is supported only for Baremetal CNE deployments. The upgrade from cnDBTier 1.8.x to 1.9.x is supported.	NA

Table 3-1 (Cont.) Media Pack Contents for Cloud Native Core 2.4.0

Description	Versions	ATS Test Cases Included	Upgrade	Compliance
Oracle Communications Cloud Native Core Cloud Native Environment (CNE)	1.9.0	NA	CNE 1.9.0 supports fresh installation. The upgrade from CNE 1.8.4 to 1.9.1 is supported only for Baremetal CNE deployments. The upgrade from cnDBTier 1.8.9 to 1.9.0 is supported.	NA
Oracle Communications Cloud Native Core Inter-Working Function (IWF)	1.5.0	NA	Supports fresh installation only	Compatible with: • BSF 1.5.0 • NRF 1.7.0 • UDR 1.7.0 • Compliant with 3GPP version 15.5
Oracle Communications Cloud Native Core Network Exposure Function (NEF)	1.3.0	No	Supports fresh installation only	Compatible with: • cnDBTier 1.8.7 • OCCNE 1.8.0 • NRF 1.10.0

Table 3-1 (Cont.) Media Pack Contents for Cloud Native Core 2.4.0

Description	Versions	ATS Test Cases Included	Upgrade	Compliance
Oracle Communications Cloud Native Core Network Repository Function (NRF)	1.14.1	Y	NRF 1.14.1 supports a fresh installation as well as upgrade from 1.12.x to 1.14.1, and 1.14.0 to 1.14.1. For more information on installation or upgrading, see *Oracle Communications Cloud Native Core Network Repository Function Installation and Upgrade Guide.*	Compatible with: • SLF 1.14.0 • cnDBTier 1.8.8, 1.9.0 • OSO 1.6.2 • OCCNE 1.9.0 • Kubernetes 1.19.7 • Network functions which are compliant with 3GPP Release: – 29.510 v15.5 (September 2019) – 29.510 v16.3.0 * Support for NFSet parameter * Support for SCP as NfType • 29.510 v16.7 – smfInfo – smfInfoList

Table 3-1 (Cont.) Media Pack Contents for Cloud Native Core 2.4.0

Description	Versions	ATS Test Cases Included	Upgrade	Compliance
Oracle Communications Cloud Native Core Network Repository Function (NRF)	1.14.0	Y **Note**: Not applicable to Failure KPIs per Service Operation:	NRF 1.14.0 supports a fresh installation as well as upgrade from 1.12.x to 1.14.0. For more information on installation or upgrading, see *Oracle Communications Cloud Native Core Network Repository Function Installation and Upgrade Guide.*	Compatible with: • SLF 1.14.0 • cnDBTier 1.8.7 (With and Without ASM) • OSO 1.6.2 • OCCNE 1.8.3 • Kubernetes 1.18.8 • Network functions which are compliant with 3GPP Release: – 29.510 v15.5 (September 2019) – 29.510 v16.3.0 * Support for NFSet parameter * Support for SCP as NfType • 29.510 v16.7 – smfInfo – smfInfoList
Oracle Communications Cloud Native Core Network Slice Selection Function (NSSF)	1.7.0	Yes	Supports fresh installation only	Compatible with: • CNE 1.8.x • CNDBTier 1.8.x • OSO 1.6.2 • Kubernetes 1.18.8 • ASM1.6.14-am4 • Compliant with 3GPP TS 29.531 version 15.5.0

Table 3-1 (Cont.) Media Pack Contents for Cloud Native Core 2.4.0

Description	Versions	ATS Test Cases Included	Upgrade	Compliance
Oracle Communications Cloud Native Core Policy (CNC Policy)	1.14.1	Yes **Note:** Not applicable to: • Support for Debug Tool • Consistent Logging Level Support	Supports fresh installation as well as upgrade from 1.12.x or 1.14.0 to 1.14.1, based on the selected mode: • **Converged Policy Mode**: In converged mode, Policy supports only fresh installation. • **PCF Mode**: In PCF mode, the installation or upgrade depends on the CNE version: – With CNE 1.9.1, Policy 1.14.1 supports fresh installation only. – With CNE 1.7.2, upgrade to Policy 1.14.1 is supported. • **PCRF Mode**: In PCRF mode, only fresh installation is supported. For more information on installation or upgrade, see *Oracle Communications Cloud Native Core Policy Installation and Upgrade Guide*	Compatible with: • NRF 1.14.0 • UDR 1.14.0 • BSF 1.10.1 • cnDBTier 1.9.1 • OSO 1.7.0 • ASM 1.6.14-am4 • CNE 1.9.1 • CNE 1.7.2

Table 3-1 (Cont.) Media Pack Contents for Cloud Native Core 2.4.0

Description	Versions	ATS Test Cases Included	Upgrade	Compliance
Oracle Communications Cloud Native Core Policy (CNC Policy)	1.14.0	Yes **Note:** Not applicable to: • Support for Debug Tool • Consistent Logging Level Support	Supports fresh installation as well as upgrade from 1.12.x to 1.14.0, based on the selected mode: • **Converged Policy Mode**: In converged mode, Policy supports only fresh installation. • **PCF Mode**: In PCF mode, the installation or upgrade depends on the CNE version: – With CNE 1.8.3, Policy 1.14.0 supports fresh installation only. – With CNE 1.7.2, upgrade to Policy 1.14.0 is supported. For more information on installation or upgrade, see *Oracle Communications Cloud Native Core Policy Installation and Upgrade Guide*	Compatible with: • NRF 1.14.0 • UDR 1.14.0 • BSF 1.10.0 • CNDBTier 1.8.7 • OSO 1.7.0 • ASM 1.6.14-am4 • CNE 1.8.3 • CNE 1.7.2
Oracle Communications Cloud Native Core Service Communication Proxy (SCP)	1.14.1	Yes	SCP 1.14.1 supports a fresh installation as well as upgrade from 1.12.x and 1.14.0 to 1.14.1. For more information about installation and upgrade, see *Oracle Communications Cloud Native Core Service Communication Proxy Installation and Upgrade Guide*.	Compatible with: • cnDBTier 1.8.7 and 1.9.1 • OSO 1.6 • OCCNE 1.7.0, 1.8.4, and 1.9.1 • Kubernetes 1.19.7 • ASM 1.6.14-am4

Table 3-1 (Cont.) Media Pack Contents for Cloud Native Core 2.4.0

Description	Versions	ATS Test Cases Included	Upgrade	Compliance
Oracle Communications Cloud Native Core Service Communication Proxy (SCP)	1.14.0	Yes	SCP 1.14.0 supports a fresh installation as well as upgrade from 1.12.0 to 1.14.0. For more information about installation and upgrade, see *Oracle Communications Cloud Native Core Service Communication Proxy Installation and Upgrade Guide*.	Compatible with: • cnDBTier 1.8.7 • OSO 1.6 • OCCNE 1.6.0, 1.7.0, and 1.8.3 • Kubernetes 1.18.8 • ASM 1.6.14-am4
Oracle Communications Cloud Native Core Security Edge Protection Proxy (SEPP)	1.6.1	No	Supports fresh installation only	Compatible with: • CNE 1.8.4, 1.8.1 • cnDBTier 1.8.0.0.3 • Kubernetes 1.18.8 • ATS 1.8.0 • CNC Console 1.8.0
Oracle Communications Cloud Native Core Security Edge Protection Proxy (SEPP)	1.6.0	Yes	Supports fresh installation only	Compatible with: • CNE 1.8.4, 1.8.1 • cnDBTier 1.8.0.0.3 • Kubernetes 1.18.8 • CNC Console 1.8.0
Oracle Communications Cloud Native Core Unified Data Repository (UDR)	1.14.0	Y	1.14.0 supports a fresh installation as well as upgrade from 1.12.x. For more information on installation or upgrading, see *Cloud Native United Data Repository Installation and Upgrade Guide*	Compatible with: Compatible with: • CNE 1.8.3 • NRF 1.14.0, PCF • cnDBTier 1.8.8 • Kubernetes 1.18.8 • OSO 1.6.x • ASM 1.6.14-am4
Oracle Communications Cloud Native Core Unified Data Management (UDM)	1.1.0	NA	Supports fresh installation only	NA

Common Services Load Lineup

This section provides information about common services supported by each network function and ATS for Cloud Native Core release 2.4.0.

Table 3-2 Common Services Load Lineup for Network Functions

Common Service	BSF	CNC Policy	NRF	NSSF	UDR	SEPP	CNC Console	SCP
Alternate Route Svc	1.5.1	1.5.1	NA	NA	1.5.1	NA	NA	NA
App-Info	1.14.1	1.14.1	1.14.1	1.14.0	1.14.0	1.14.0	NA	NA
ASM Configuration	1.0.0	1.0.0	1.6.14.am-4	1.6.14.am-4	1.6.14-am4	NA	NA	1.6.14-am4
ATS Framework	1.8.0	1.8.0	1.8.0-p25-1	1.8.0	1.8.0	1.8.0	NA	1.8.0
Config-Server	1.14.1	1.14.1	NA	1.14.0	1.14.0	1.14.0	NA	NA
Debug-tool	1.1.0	1.1.0	1.1.0	1.1.0	1.1.0	NA	1.1.0	1.1.0
Egress Gateway	1.14.6	1.14.6	1.14.6	1.14.3	1.14.2	1.14.3	1.14.6	NA
Ingress Gateway	1.14.6	1.14.6	1.14.6	1.14.3	1.14.3	1.14.3	1.14.6	NA
Helm Test	1.14.1	1.14.1	1.14.1	1.14.1	1.14.1	NA	1.14.1	1.14.1
NRF-Client	1.8.1	1.8.1	NA	1.8.0	1.8.0	1.8.0	NA	NA
Perf-Info	1.14.1	1.14.1	NA	1.14.0	1.14.0	1.14.0	NA	NA

Security Certification Declaration

The following table lists the security tests and the corresponding dates of compliance for each network function.

Table 3-3 Security Certification Declaration

Compliance Test Description	BSF	CNC Policy	NRF	NSSF	UDR	SEPP	CNC Console	SCP
Systems test on functional and security features	NA	NA	NA (No new security feature)	NA	NA (No new security feature)	NA (No new security feature)	NA (No new security feature)	NA
Regression testing on security configuration	NA	NA	August 10, 2021	NA	August 13, 2021	October 20, 2021 (ATS test cases)	October 8, 2021	NA
Vulnerability testing	August 21, 2021	August 21, 2021	August 10, 2021	August 11, 2021	August 13, 2021	October 20, 2021	October 8,2021	August 19, 2021

Table 3-3 (Cont.) Security Certification Declaration

Compliance Test Description	BSF	CNC Policy	NRF	NSSF	UDR	SEPP	CNC Console	SCP
Fuzz testing on external interfaces	August 21, 2021	August 21, 2021	August 10, 2021	August 11, 2021	August 13, 2021	August 13, 2021	October 8, 2021	August 17, 2021

Documentation Pack

All documents for Cloud Native Core (CNC) 2.4.0 are available for download on SecureSites and MOS.

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

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

4

Resolved and Known Bugs

This chapter lists the resolved and known bugs for Cloud Native Core release 2.4.0.

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.

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.

Resolved Bug List

The following Resolved Bugs tables list the bugs that are resolved in Cloud Native Release 2.4.0.

BSF Resolved Bugs

Table 4-1 BSF 1.10.1 Resolved Bugs

Bug Number	Severity	Found in Release	Title
33459045	3	1.7.2	Prometheus issue in functional lab
33459109	3	1.9.0	Diameter Peer in GR setup keeps going down
33459148	3	1.9.0	Policy and BSF installation is not working

Table 4-2 BSF 1.10.0 Resolved Bugs

Bug Number	Severity	Found in Release	Title
33132080	3	1.9.0	Failed to remove the diam connection when the last peer node configuration is deleted
32377395	3	1.7.0	occnp_diam_conn_backend measurement is incremented for {appType="pcf",} for bsf

CNC Console Resolved Bugs

Table 4-3 CNC Console 1.8.1 Resolved Bugs

Bug Number	Severity	Found in Release	Title
33316527	4	1.7.0	Unable to open Common Services component GUI through CNCC
33316539	4	1.7.0	Policy project deletion not happening through CNCC GUI
33446327	4	1.7.0	Modifying SiteID to SiteName in NRF (CNCC GUI) and custom yaml

Table 4-4 CNC Console 1.8.0 Resolved Bugs

Bug Number	Severity	Found in Release	Title
33173804	Minor	1.6.1	VzW _CNCC test pod comes up before the application pods
32291223	Minor	1.5.0	CNCC: CNE Common Services type should be ClusterIP when accessed via CNCC
33157991	Minor	1.7.0	Update custom annotation for Metallb address pool in CNE environment

CNE Resolved Bugs

Table 4-5 cnDBTier 1.9.2 Resolved Bugs

Bug Number	Severity	Found in Release	Title
33398973	2	1.8	cnDBTier 1.9.2 GA build to VzW with MySQL NDB bug fixes
33237783	2	1.8	cnDBTier 1.9.2 GA build to VzW with MySQL NDB bug fixes
32820167	3	1.8	cnDBTier 1.9.2 GA build to VzW with MySQL NDB bug fixes
33488981	2	1.9	cnDBTier install without ndbapp sql nodes i.e. ndbappReplicaCount as 0
33488770	2	1.9	cnDBTier ndbapp pods are not replicating the user details and grants

Table 4-6 CNE 1.9.1 Resolved Bugs

Bug Number	Severity	Found in Release	Title
33405874	2	1.9.0	Kubespray fails installing K8s on OpenStack with TLS enabled
33431094	2	1.9.0	Container registry configuration needs update to handle some K8S containers
33431127	2	1.9.0	Missing parameter: type definition for Storage Class occne-metrics-sc
33431152	2	1.9.0	Post deployment observing no mount for Openstack certificate in lb controller pod
33431161	2	1.9.0	Remove subnetname from lb_controller
33431186	3	1.9.0	Update VM naming convention
33445871	2	1.9.0	createFailedLbvm.py and addPeerAddrPools.py script failures

Table 4-7 cnDBTier 1.9.1 Resolved Bugs

Bug Number	Severity	Found in Release	Title
33393988	4	1.9.0	Provide support for old prometheus alert in cnDBTier
33410333	3	1.9.0	Correct annotation placement in dbparams.ini file

Table 4-8 CNE 1.9.0 Resolved Bugs

Bug Number	Severity	Found in Release	Title
33355833	2	1.9	Allow ES curator to continue if individual steps fail
33355862	2	1.9	kubelet service is not using latest changes

Table 4-9 cnDBTier 1.9.0 Resolved Bugs

Bug Number	Severity	Found in Release	Title
33352224	3	1.8	db backup svc sometimes not removing the backup directory after marking the backup id as purged
33352881	4	1.9	Continuous ERROR messages are printed in monitor svc when replication is not configured
33352911	3	1.8	Replication Channel information is partially loading into the cnDBTier replication service
33352927	3	1.8	Getting "No operations allowed after connection closed" for replication svc

NRF Resolved Bugs

Table 4-10 NRF 1.14.1 Resolved Bugs

Bug Number	Severity	Found In Release	Title	Customer Impact
33446224	4	1.12.1	OcnrfDbReplicationStatusInactive Alert not firing even if NRF detected replication is down	When replication goes down, Operator will not see alarm regarding it.

Table 4-10 (Cont.) NRF 1.14.1 Resolved Bugs

Bug Number	Severity	Found In Release	Title	Customer Impact
33446277	4	1.14.0	Correct the indentation for ingress-gateway and egress-gateway actuator port in umbrella values.yaml file	If Custom Value is not used for deployment, then there will be no impact
33446327	4	1.14.0	Modifying SiteID to SiteName in CNCC GUI and REST	Name SiteID is misleading, SiteName should be configured instead
33446378	4	1.14.0	Default value in "replicationStatusUri" should be "http://occne-db-monitor-svc:3306/db-tier/status/replication"	NRF will not be able to detect replication is down due to wrong URI

Table 4-11 NRF 1.14.0 Resolved Bugs

Bug Number	Severity	Found In Release	Title	Customer Impact
32973074	4	1.12.0	GET All API is not returning siteIdToNrfInstanceIdMappingList configuration values	During Backup, apart from doing GET All API to collect the configuration, additionally, siteIdToNrfInstanceIdMappingList backup needs to be taken.
32973081	4	1.12.0	ocnrf_heartbeat_missed_total counter gets pegged erroneously in SUSPENDED -> REGISTERED case	Incorrect Metric value will be seen for Heart Beat missed for NFs moving from Suspended to Registered. No other functionality will be effected.
32973027	4	1.12.0	Invalid Via header port value returns 500 internal error instead bad request	Response with incorrect HTTP Status code will be sent to consume NF
33245249	4	1.14.0	NFDiscover plmn-specific-snssai-list query is not returning matching NFProfile	Discovery with plmn-specific-snssai-list will not return NfProfiles even if there are matching perPLMNSnssai present
33245263	4	1.11.1	NRF fails to send notification to subscriber for profiles with more than one entry in nfSetIdList	Consumer NF will not get notified for NFs with more than one nfSetId in nfSetIdList

Table 4-11 (Cont.) NRF 1.14.0 Resolved Bugs

Bug Number	Severity	Found In Release	Title	Customer Impact
33245279	4	1.11.1	nfManagementOptions allowDuplicateSubscriptions can't be set to true once set to false	Operator can't change allowDuplicateSubscriptions configuration value alone. As a workaround, If the parameter is set to true along with other parameter in nfManagementOptions, then it will allow.
33245340	4	1.12.0	OCNRF considers PLMNID with 2 digit MNC and same PLMNID with 3 digit MNC with a leading 0 as different PLMN.	While Querying to NRF, PLMNID value needs to be sent with same format that is there in the NfProfile. Otherwise the query will result no match.
33245421	3	1.14.0	Initiator OCNRF is encoding Discovery Query with array of object attributes (e.g. target-plmn-list) incorrectly while forwarding the request to target NRF	Forwarding of Discovery query with array of object attributes (e.g. target-plmn-list) will always be rejected by target NRF with 4xx code.

NSSF Resolved Bugs

Table 4-12 NSSF 1.7.0 Resolved Bugs

Bug Number	Severity	Found in Release	Title
33172166	2	1.6	CVE-2021-3426: PYTHON UPDATE TO AT LEAST 3.9.3, 3.8.9, 3.7.11 OR 3.6.14
33135303	3	1.6	Critical CVEs Identified in ocats-nssf using Anchore Security Scan

CNC Policy Resolved Bugs

Table 4-13 CNC Policy 1.14.1 Resolved Bugs

Bug Number	Severity	Found In Release	Title
33459222	3	1.12.0	Policy and BSF installation is not working
33459267	3	1.12.0	Bulk Import is not working properly in cnPCRF
33459271	3	1.14.0	Timer profile export fails with Bulk Export Operation

Table 4-13 (Cont.) CNC Policy 1.14.1 Resolved Bugs

Bug Number	Severity	Found In Release	Title
33459310	3	1.12.0	SM PCF cnDBTier 1.8.8 db replication failure
33463586	2	1.12.3	SW block "Remove all from Subscriber Remote" does not work - delete fails

Table 4-14 CNC Policy 1.14.0 Resolved Bugs

Bug Number	Severity	Found In Release	Title
32650916	2	1.11.3	Diamgw throws "No OCS/SH peer to send msg" even when it connected successfully
32995443	3	1.11.2	PCF sends PATCH request to UDR even in the absence of policies
32995086	3	1.11.0	ASA message is not sent to backend but back to peer
32995076	3	1.11.0	1.12.0 cmgui has configurations related to disabled services in pcrf mode.
32995073	3	1.11.0	UDR Notification for Multiple Resources is not handled by PCF
32650928	3	1.11.0	Pcrf-core should send the binding data entry and pds entry delete request after diameter session deletion.
32995081	3	1.12.0	Memory leak in diam-connector when diam-gw pod scales
33130516	3	1.11.4	PCF User Connector - base URI changes via GUI not taking affect
33159055	3	1.11.4	PCF unable to read UDR connector service configuration change
33131466	3	1.11.4	Diameter Peer Node Configuration FQDN validation issue during Bulk Import/Export
33223451	3	1.11.4	PCF sending NULL smPolicyDecision in audit messages

SCP Resolved Bugs

Table 4-15 SCP 1.14.1 Resolved Bugs

Bug Number	Severity	Found in Release	Title
33460911	3	1.14.0	Application User missing NDB_STORED_USER permissions
33460920	4	1.14.0	Document update for privileged user permissions

Table 4-15 (Cont.) SCP 1.14.1 Resolved Bugs

Bug Number	Severity	Found in Release	Title
33460931	3	1.14.0	Audit microservice upgrade failure due to namespace and releasename variable missing in upgrade hooks
33460935	3	1.14.0	Duplicate rules creation on scp worker pod restart
33460944	3	1.14.0	Hostmpper null pointer exception observed in scp worker
33460956	4	1.14.0	Enable R15 as input to New features ATS
33460975	4	1.14.0	Fix comments in ATS custom deployment file
3465417	3	1.12.0	Add Pod scale up in cleanup of NRF Registration feature file

Table 4-16 SCP 1.14.0 Resolved Bugs

Bug Number	Severity	Found in Release	Title
33233332	3	1.11.1	Update Rate limiting scenarios to remove validation from cleanup scenario
33233343	4	1.12.0	Remove IGW images and charts in CSAR package for SCP 1.10.x onward releases
33233454	4	1.11.1	Perform validation of microservice names for logger API
33233561	4	1.12.0	Change Timestamp format for all logs to "2021-06-18T19:07:01.329+0000"
33249040	3	1.11.0	Under high traffic SCP keeps on processing requests even if connections are terminated
33233542	4	1.12.0	Add complete ats custom config templates content to ATS CSAR pacakage

SEPP Resolved Bugs

Table 4-17 SEPP 1.6.1 Resolved Bugs

Bug Number	Severity	Found in Release	Title
33264360	2	1.5.0	Multipart message is not supported in SEPP
33263736	2	1.5.0	cn32f crashed during stress testing
33486560	2	1.5.0/ 1.6.0	Roaming NRF Discovery error at egress level

Table 4-17 (Cont.) SEPP 1.6.1 Resolved Bugs

Bug Number	Severity	Found in Release	Title
33373718	2	1.5.0/ 1.6.0	Media type payload is getting changed when passing from vSEPP to hSEPP

Table 4-18 SEPP 1.6.0 Resolved Bugs

Bug Number	Severity	Found in Release	Title
33163603	2	1.4.0	Discovery Procedure is failing for query parameter
33160425	2	1.5.0	Query parameters of NRF discovery are removed by the SEPP n32f proxy
33160382	3	1.5.0	SEPP 1.5.0 MIBs Not Compiled Correctly
33118522	3	1.5.0	IP Based routing in absence of External DNS
33118491	2	1.5.0	Multiple values not supported in SAN
33184851	3	1.5.0	Roaming Partner Profile not getting deleted when the connection type is Responder

UDR Resolved Bugs

Table 4-19 UDR 1.14.0 Resolved Bugs

Bug Number	Severity	Found in Release	Title
32972133	3	1.12.0	Notify pod not sending notifications every time to the stub for PATCH of sdmsubscription
32377341	4	1.10.0	Fetch UDM authentication subscription on UDR returns Internal Server Error

Customer Known Bug List

Customer Known Bugs tables list the known bugs and associated Customer Impact Statements. This information is provided for information purposes only.

BSF Customer Known Bugs

Table 4-20 BSF 1.10.0 Customer Known Bugs

Bug Number	Severity	Found in Release	Title	Customer Impact
33262764	3	1.9.0	Ephemeral storage requirement for BSF	In absence of ephemeral storage requirement underlying HW will not reserve space for the BSF pods and pods can get evacuated if the storage space is not available
33262827	3	1.10.0	Default selection not seen and Export button enabled though there is no selection on Bulk Export modal	User needs to select the configuration that are needed for export
33263632	3	1.10.0	BSF SBI HTTP Error codes are not allowing custom error codes	Only Standard HTTP status code are allowed

CNC Console Customer Known Bugs

There are no customer known bugs in CNC Console 1.8.x.

CNE Customer Known Bugs

Table 4-21 CNE 1.9.0 Customer Known Bugs

Bug Number	Severity	Found in Release	Title	Customer Impact
32211087	2	1.4	nodename field is blank for CNE node alerts OUT_OF_MEMORY and NODE_UNAVAILABLE	The nodename field remains blank for the following CNE node alerts: • OUT_OF_MEMORY • NODE_UNAVAILABLE
33356061	3	1.4	Modify NETWORK_INTERFACE_FAILED alert to fire separate alert for gen10 and gen8 h/w	The current definition of NETWORK_INTERFACE_FAILED alert sends a false alarm for gen10 hardware.
33356081	4	1.6	vCNE/Metallb - genLbCtrlData.py script fails using IP ranges	When the `genLbCtrlData.py` script is run to generate the `lbCtrlData.json` file, it fails to add network id and other fields to the json file.

Table 4-21 (Cont.) CNE 1.9.0 Customer Known Bugs

Bug Number	Severity	Found in Release	Title	Customer Impact
33353135	3	1.9	virtual CNE 1.9 upgrade ends with unattached cinder volumes causing outage	virtual CNE 1.9 upgrade ends with unattached cinder volumes, causing outage
33353123	3	1.9	1.9.0-rc.7 Fixed IP vCNE Install failure	The current Fixed IP install fails in the `deploy.sh` script.

NRF Customer Known Bugs

Table 4-22 NRF 1.14.0 Customer Known Bugs

Bug Number	Severity	Found in Release	Title	Customer Impact
33248344	4	1.14.0	slfOptions.featureStatus is accepting invalid values if CLI based REST client is used	The issue will occur only if CLI based REST client is used to enable SLF feature with an invalid value. With CNC Console GUI, this issue will never occur.

NSSF Customer Known Bugs

There are no customer known bugs in NSSF Release 1.7.0.

CNC Policy Customer Known Bugs

Table 4-23 CNC Policy 1.14.0 Customer Known Bugs

Bug Number	Severity	Found in Release	Title	Customer Impact
33263619	3	1.14.0	UDR/CHF updated binding header is not picked in routing binding header while sending Update/Unsubscribe request to UDR/CHF	If UDR or CHF updates its binding information in Update Response message or Notification request message, PCF will not honour the updated binding and shall continue to use the binding information received in Subscribe response in the Routing Binding Header while sending Update and Unsubscribe request to UDR or CHF.

Table 4-23 (Cont.) CNC Policy 1.14.0 Customer Known Bugs

Bug Number	Severity	Found in Release	Title	Customer Impact
33263638	3	1.14.0	Binding header is sent every time in UDR notification response even if NFSet of PCF is not changed	Extra header will be sent to HTTP peers but will not cause any functionality loss.
33131318	3		PCF SM service calling alternate route service on subsequent requests	This issue occurs when the Retry Profile is configured and DNS SRV records are not created. This can be avoided by performing the following steps: 1. Remove the retry profile configuration from SM Service configuration (If customer does not want the Alt Routing for SMF Notification) 2. If Alternate Routing is required then configure the DNS SRV records
33218137	3	1.12.0	BULK Export operation skips default service configuration during export	Default Service configuration is not exported unless it is saved at least once from the GUI. This will result in Bulk Export operation skipping the Service Configuration data.
33263667	3	1.12.0	Ephemeral storage requirement for CNC Policy	In absence of ephemeral storage requirement underlying hardware will not reserve space for the Policy pods and pods can get evacuated if the storage space is not available.

SCP Customer Known Bugs

There are no customer known bugs in SCP Release 1.14.0.

SEPP Customer Known Bugs

SEPP 1.6.1 Customer Known Bugs

Table 4-24 SEPP 1.6.1 Customer Known Bugs

Bug Number	Severity	Found in Release	Title	Customer Impact
33322009	3	1.6.1	Cache not getting updated for deleted entries.	If Roaming Partner Profile is deleted and n32f traffic is in progress, n32f will keep on finding the context and continue forwarding the message to receiving SEPP.
33323304	3	1.6.1	DB operations taking approximately 60 seconds to reflect in N32f services.	If N32f traffic is run immediately after performing any DB update related to Roaming Partner Profile (create or update), N32f message fails with 404 -Context not found error message.

SEPP 1.6.0

There are no customer known bugs in SEPP Release 1.6.0

UDR Customer Known Bugs

Table 4-25 UDR 1.14.0 Customer Known Bugs

Bug Number	Severity	Found in Release	Title	Customer Impact/WA
30774742	4	1.3.0	UDR is not validating the conditional attributes for UDM APIs.	No impact. UDM(consumer of UDM APIs) does not send conditional attributes to UDR
30774750	4	1.3.0	Notify Service delays notifications to PCF during traffic run	Notifications rate is limited in initial release.
30774755	3	1.4.0	Headers for few resources are not implemented as per spec 29505-v15.4.0	No impact.
32377439	4	1.10.0	De-Registration fails when egress gateway goes down before nrf-client during UDR deletion	No impact