Oracle® Communications

Cloud Native Core Release Notes

Release 2.3.4
F43832-17
November 2021

Oracle Communications Cloud Native Core Release Notes, Release 2.3.4

F43832-17

Contents

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 2.3.4 in Oracle Communications Cloud Native Core (CNC) Release Notes.

Release 2.3.4 - F43832-17, November 2021

NEF Release 1.3.1

The following sections are updated for NEF Release 1.3.1:

- Network Exposure Function (OCNEF): Added new enhancements
- Media Pack: Added Media pack details

Release 2.3.4 - F43832-16, September 2021

SCP Release 1.12.1

The following sections are updated for SCP Release 1.12.1:

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

Release 2.3.4 - F43832-15, September 2021

CNC Policy Release 1.12.3

The following sections are updated for CNC Policy Release 1.12.3:

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

Release 2.3.4 - F43832-14, August 2021

CNC Policy Release 1.12.2

The following sections are updated for CNC Policy Release 1.12.2:

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

Release 2.3.4 - F43832-13, July 2021

CNC Console Release 1.7.2

The following sections are updated for CNC Console Release 1.7.2:

- CNC Console Resolved Bugs: Added resolved bugs list
- CNC Console Customer Known Bugs: Added customer known bugs list

Release 2.3.4 - F43832-12, July 2021

BSF Release 1.9.1

The following sections are updated for BSF Release 1.9.1:

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

Release 2.3.4 - F43832-11, July 2021

CNC Policy Release 1.12.1

The following sections are updated for CNC Policy Release 1.12.1:

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

Release 2.3.4 - F43832-10, July 2021

NRF Release 1.12.1

The following sections are updated for NRF Release 1.12.1:

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

Release 2.3.4 - F43832-09, July 2021

Updated the Media Pack details for Policy 1.12.0.

Release 2.3.4 - F43832-08, July 2021

UDR ATS Release 1.12.1

The following sections are updated for UDR ATS Release 1.12.1:

- 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

Release 2.3.4 - F43832-07, June 2021

SCP Release 1.12.0

The following sections are updated for SCP Release 1.12.0:

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

Release 2.3.4 - F43832-06, June 2021

CNC Console Release 1.7.1

The following sections are updated for CNC Console Release 1.7.1:

- 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 Customer Known Bugs: Added customer known bugs list

Release 2.3.4 - F43832-05, June 2021

Updated the Common Services Load Lineup section.

Release 2.3.4 - F43832-03, June 2021

BSF 1.9.0

The following sections are updated for CNC Policy 1.12.0:

- Binding Support Function (BSF): Added new features/enhancements
- Media Pack: Added Media pack details
- Security Compliance Information: Added Security Compliance Information
- BSF Resolved Bugs: Added resolved bugs list

CNC Policy 1.12.0

The following sections are updated for CNC Policy 1.12.0:

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

Release 2.3.4 - F43832-02, June 2021

CNC Console Release 1.7.0

The following sections are updated for CNC Console Release 1.7.0:

- Cloud Native Core Console (CNC Console): Added new features/enhancements
- Media Pack: Added Media pack details
- Common Services Load Lineup section.
- Security Compliance Information: Added Security Compliance Information
- CNC Console Resolved Bugs: Added resolved bugs list
- CNC Console Customer Known Bugs: Added customer known bugs list

NRF Release 1.12.0

The following sections are updated for NRF Release 1.12.0:

- 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 1.6.0

The following sections are updated for NSSF Release 1.6.0:

- 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

UDR Release 1.12.0

The following sections are updated for UDR Release 1.12.0:

- 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

Release 2.3.4 - F43832-01, June 2021

NEF Release 1.3.0

The following sections are updated for NEF Release 1.3.0:

- Media Pack: Added Media pack details
- Security Complaince Information: Added Security Compliance Information

SEPP Release 1.5.0

The following sections are updated for SEPP Release 1.5.0:

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

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 2.3.4.

Automated Testing Suite (ATS)

There are no new features or updates implemented in CNC 2.3.4 release.

Binding Support Function (BSF)

Binding Support Function (BSF) 1.9.0 is updated with the following enhancements:

- **Three-Site Georedundancy:** BSF is enhanced to support the three-site Geographical Redundant (Georedundant) deployment. It offers, both three-site and two-site georedundancy to ensure service availability when one of the BSF sites is down. For more information, see "Georedundancy Support" in *Oracle Communications Cloud Native Binding Support Function User's Guide*.
- **Overload Control and Handling - SBI - phase 1:** BSF supports overload management to prevent the performance of services from degrading, in an uncontrolled fashion under heavy load, using BSF REST APIs. For more information about the Overload Control and Handling, see "Overload Control and Handling - SBI " in *Oracle Communications Cloud Native Binding Support Function User's Guide*.
- **Support for ASM Helm Config:** With this feature, orchestration of CNC Policy along with ASM resource configurations has been automated. Resources, such as PeerAuthentication, ServiceEntry, DestinationRule, and EnvoyFilter can be configured in an automated way, using ASM data plane configuration helm chart. For more information, see *Oracle Communications Cloud Native Binding Support Function Installation Guide*.
- **NF Set Registration:** With this feature, each instance of BSF registers the NF Set with Network Repository Function, so that Service Communication Proxy (SCP) can perform the Alternate Routing. For more information, see "NRF Client Configuration" in *Oracle Communications Cloud Native Binding Support Function Installation Guide*.

Cloud Native Core Console (CNC Console)

Cloud Native Core Console (CNC Console) 1.7.1 has been updated with the following enhancement:

- **GUI Support the lastet version of SCP:** CNCC GUI support for the latest version of SCP (1.12.0).

Cloud Native Core Console (CNC Console) 1.7.0 has been updated with the following enhancements:

- **OJET upgrade**: CNC Console backend OJET is upgraded to the latest version, which enhances the GUI look and feel.

- **Integration with Aspen service mesh (ASM) 1.6.14-am4**: Oracle CNC Console leverages the Istio or Envoy service mesh for all internal and external communication. ASM Version is updated to ASM 1.6.14-am4. For more information, see *Oracle Communications Cloud Native Core Console Installation and Upgrade Guide*.
- **Support the latest version of NFs**: CNC Console is compatible with the latest version of the supported NFs:
  - SCP 1.12.0
  - NRF 1.12.0
  - UDR 1.12.0
  - POLICY 1.12.0
  - BSF 1.9.0

Cloud Native Core Policy (CNC Policy)

CNC Policy 1.12.1

Oracle Communications Cloud Native Core Policy (CNC Policy) 1.12.1 has been updated with the following enhancements:

- **Enhancement 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*.

CNC Policy 1.12.0

Oracle Communications Cloud Native Core Policy (CNC Policy) 1.12.0 has been updated with the following enhancements:

- **Three-Site Georedundancy:** CNC Policy is enhanced to support the three-site Geographical Redundant (Georedundant) deployment. It offers, both 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's Guide*.
- **Export of Policies with Dependencies using GUI:** CNC Policy is enhanced to support bulk export of Policy Managed Objects (MOs) and Policy Projects with their dependencies using CNC Console. For more information on the GUI enhancements, see "Import & Export" in *Oracle Communications Cloud Native Core Policy User's Guide*.
- **Overload Control and Handling - SBI - phase 1:** CNC Policy supports overload management to prevent the performance of the Policy services from degrading in an uncontrolled fashion under heavy load, using Policy REST APIs. For more information about Overload Control and Handling, see "Overload Control and Handling - SBI" in *Oracle Communications Cloud Native Core Policy User's Guide*.
- **Support for ASM Helm Config:** With this feature, orchestration of CNC Policy along with ASM resource configurations has been automated. Resources such as PeerAuthentication, ServiceEntry, DestinationRule, and EnvoyFilter can be configured in an automated way using ASM data plane configuration helm chart. For more information, see "Aspen Service Mesh Configurations" in *Oracle Communications Cloud Native Core Policy Installation and Upgrade Guide*.

- **NF Set Registration:** With this feature, each instance of CNC Policy registers the NF Set with Network Repository Function (NRF), so that Service Communication Proxy (SCP) can perform Alternate Routing. For more information, see "NRF Client Configuration" in *Oracle Communications Cloud Native Core Policy Installation and Upgrade Guide*.
- **Handling of Stale Session Notification in PCRF-Core:** With this enhancement, PCRF Core service is integrated with audit service. Using CNC Console, audit service related configurations can be done for Gx and Rx diameter sessions. For more information, see "Configuring CNC Policy using CNC Console" in *Oracle Communications Cloud Native Core Policy User's Guide*.
- **Notification Handling from PDS for PCRF-Core:** With this enhancement, PCRF Core service will be able to process only update notification requests from nUDR and LDAP. Based on the requests, policy evaluation is done and appropriate policy rules are installed. For more information, see "Notification Handling from PDS for PCRF-Core" in *Oracle Communications Cloud Native Core Policy User's Guide*.
- **Enhancement 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*.
- **OJET Upgrade:** The CNC Console backend OJET is upgraded to the latest version, which enhances the GUI look and feel.

Cloud Native Diameter Routing Agent (CnDRA)

There are no new features or updates implemented in CNC 2.3.4 release.

Cloud Native Environment (CNE)

There are no new features or updates implemented in CNC 2.3.4 release.

CNC NF Data Collector

There are no new features or updates implemented in CNC 2.3.4 release.

Inter-Working Function (IWF)

There are no new features or updates implemented in CNC 2.3.4 release.

Service Communication Proxy (SCP)

SCP 1.12.1 has been updated with the following enhancement:

- 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*.

SCP 1.12.0 has been updated with the following enhancements:

- **Support for Multus Container Network Interface**: SCP uses Multus Container Network Interface (CNI) plug-in to connect multiple network interfaces to pods in Kubernetes. After integrating Multus CNI with SCP, multiple interfaces can be created in a pod. For more

information about the feature, see *Oracle Communications Cloud Native Core Service Communication Proxy (SCP) User's Guide*.

- **Support for Model C Indirect 5G SBI Communication**: SCP uses Release 16 of Model C Indirect 5G SBI Communication format to enable consumer NFs to route service requests to producer NFs through SCP. For more information about the feature, see *Oracle Communications Cloud Native Core Service Communication Proxy (SCP) User's Guide*.
- **SCP ATS Enhancements**: SCP ATS has been enhanced with the following:
  - Test Case Mapping to features and Display Total Counts-New features
  - Application Logs collection on rerun

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

Security Edge Protection Proxy (SEPP)

Security Edge Protection Proxy (SEPP) 1.5.0 has been updated with the following enhancements:

- **SEPP support for Pod Tolerations and Node Selector :** This feature pins the SEPP pods to a dedicated worked node by using node selector and pod toleration. While the node selector pins the SEPP pods to the dedicated worker node, the pod tolerations ensure that other NF pods do not use the worker node dedicated for SEPP. For more information about the configuration and customization of the enhancement, see *Oracle Communications Cloud Native Core Security Edge Protection Proxy (SEPP) Installation Guide.*
- **SEPP Integration with cnDBTier 1.8.0.:** SEPP is now integrated with cnDBTier 1.8.0 in a containerized Oracle Communications Cloud Native Environment 1.8.1. For more information, see *Oracle Communications Cloud Native Core Security Edge Protection Proxy (SEPP) Installation Guide.*

Network Exposure Function (OCNEF)

OCNEF 1.3.1 has been updated with the following enhancement:

- **OCNEF Reformed Architecture:** The OCNEF architecture has been reformed with the 3GPP defined services and components. For more information about OCNEF 1.3.1 architecture, see *Oracle Communications Cloud Native Core Network Exposure Function User Guide*.
- **Helm Based Configuration:** OCNEF supports the helm based deployment model and provides the option to customize the deployment using the Custom Value file. For more information about OCNEF installation, see *Oracle Communications Cloud Native Core Network Exposure Function Installation Guide*
- **API Invoker Onboarding and Offboarding:** OCNEF supports the API Invoker Onboarding and Offboarding functionality to manage the exposure of the service APIs to different applications. For more information about the feature, see *Oracle Communications Cloud Native Core Network Exposure Function User Guide*.
- **Security Token Generation**: OCNEF supports the OAuth security method for service API invocation. This security procedure ensures that only authenticated service requests are directed to OCNEF for secures processing the requests. For

more information about the feature, see *Oracle Communications Cloud Native Core Network Exposure Function User Guide*.

- **Location Reporting:** OCNEF provides the Location Reporting functionality to provide the current or last known location of UEs in 5G network. For more information about the feature, see *Oracle Communications Cloud Native Core Network Exposure Function User Guide*.

Network Repository Function (NRF)

ATS for OCNRF 1.12.1 has been updated with a script to clean up SUT configuration if previous ATS pipeline got aborted. For more information, see *Oracle Communications Cloud Native Core Automated Test Suite Guide*.

OCNRF 1.12.0 has been updated with the following enhancement:

- **Three site geo-redundancy:** OCNRF is enhanced to support three-sites geographical redundant (georedundant) deployment. It offers both three-sites and two-sites georedundancy to ensure service availability when one of the OCNRF sites is down. For more information about georedundancy, see *Oracle Communications Cloud Native Core Network Repository Function User's Guide*.
- **OCNRF Support for IPv6 (Single Stack):** OCNRF supports communication on IPv6 addresses. OCNRF support ***IPv6 addresses, IPv6 prefix*** , and ***IPv6 Prefix Ranges*** as defined in 3GPP TS 29.571 and 3GPP TS 29.510. For more information about IPv6 support, see *Oracle Communications Cloud Native Core Network Repository Function Installation and Upgrade Guide*.
- **OCNRF support for Routing Indicator based SLF request:** OCNRF supports more flexible NF configuration for discovery query with exception list. For more information about SLF lookup, see *Oracle Communications Cloud Native Core Network Repository Function User's Guide*.
- **Support for SIDF Registration and Discovery:** OCNRF supports UDM registration, subscription, and discovery on the basis of service-name "Nudm-sucideconceal".

Network Slice Selection Function (NSSF)

OCNSSF 1.6.0 has been updated with the following enhancements:

- **Indirect communication support for NSSF:** In indirect mode of communication, consumers and producers interact through SCP. The following two communication models are supported:
  - **Model C** - Indirect communication without delegated discovery.
  - **Model D** - Indirect communication with delegated discovery.

  For more information about communication models helm parameters, see *Oracle Communications Cloud Native Core Network Slice Selection Function Installation Guide*.

  For more information on the feature description and REST API, see *Oracle Communications Cloud Native Core Network Slice Selection Function User's Guide*.
- **IPV6 Support for NSSF:** NSSF supports IPv6 addresses for its interfaces. For more information, see *Oracle Communications Cloud Native Core Network Slice Selection Function Installation Guide*.
- **Automatic DB Application User Creation:** Along with a privilege user, NSSF supports applicationUser for database access, apart from privileged user. NSSF provides a helm

option to create an application user based on the configurable parameter (`global.ocnssfHookImage.createUser`). When the helm parameter is set to true, ApplicationDbUser is created automatically. For more information, see *Oracle Communications Cloud Native Core Network Slice Selection Function Installation Guide*.

- **Integration with Aspen service mesh (ASM) 1.6.14-am4**: NSSF leverages the Istio or Envoy service mesh for all internal and external communication. ASM version is updated to ASM 1.6.14-am4. For more information, see *Oracle Communications Cloud Native Core Network Slice Selection Function Installation Guide*.
- **Pod Affinity and Anti Affinity:** NSSF has updated pod affinity and anti-affinity rules to check if all the service pods replicas are not spawned at the same node. This provides high availability when a node is down.

Unified Data Management (UDM)

There are no new features or updates implemented in CNC 2.3.4 release.

Unified Data Repository (UDR)

UDR 1.12.0 has been updated with the following enhancements:

- **Multiple Site Redundancy:** UDR or SLF supports multiple site redundancy using the cnDBTier multisite deployment model. All sites of UDR are active and can handle traffic. The replication of database is handled by configuring DBTier for multiple site deployment.

  For more information about multisite setup, see "Creating Database User or Group" in *Oracle Communications Cloud Native Core Unified Data Repository Installation and Upgrade Guide*.

  For more information about multiple site redundancy, see "Multiple Site Redundancy" feature description in *Oracle Communications Cloud Native Core Unified Data Repository User Guide*.
- **Oauth 2.0 Configuration:** Oauth 2.0 is a security feature provided to authenticate requests from valid consumer NFs. The consumer NFs request access token from the issuer, that is NRF, for a particular producer NF and uses this access token to send request to the respective producer NF.

  For more information about Oauth 2.0 feature, see "Oauth 2.0" in *Oracle Communications Cloud Native Core Unified Data Repository User Guide*.
- **KeyID Enhancement Integration:** UDR integration in CNC Console is enhanced with the introduction of KeyID. Using CNC Console, the UDR users can configure KeyID in the Access Token Validation page. For more information on how to configure access tokens, see "Access Token Validation" section in *Oracle Communications Cloud Native Core Unified Data Repository User Guide*.
- **MGM APIs for UDM and SLF Data:** MGM APIs allows the user to update the schema of UDM and SLF data stored on UDR. For more information about MGM APIs, see *Oracle Communications Cloud Native Core Unified Data Repository REST Specification Guide*.
- **IPv6 Support:** UDR or SLF supports IPv6 addresses for its interfaces. For more information, see the "Configuring Unified Data Repository" section in *Oracle*

Communications Cloud Native Core Unified Data Repository Installation and Upgrade Guide.

- **SLF ATS Lightweight Performance:** Using this feature, the SLF ATS users can run performance test cases in Jenkins. For more information about SLF-ATS Lightweight Performance feature, see the "Executing UDR Test Cases using ATS" in *Oracle Communications Cloud Native Core Automated Test Suite Guide*.

3
Media and Documentation

Media Pack

This section lists the media package for Cloud Native Core 2.3.4. 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 2.3.4

Description	Versions	ATS Test Cases Included	Upgrade	Compliance
Oracle Communications Cloud Native Core Automated Testing Suite (ATS)	1.7.0		Supports fresh installation only	UDR ATS 1.12.1 is compatible with: • CNE 1.7.x, CNE 1.8.0, CNE 1.8.1 • cnDBTier: 1.8.0.0.1, 1.8.0.0.3, 1.8.5 • OSO: 1.6.x • ASM: 1.6.14-am4
Oracle Communications Cloud Native Core Binding Support Function (BSF)	1.9.0	Yes **Note:** Not applicable to: • Support for Debug Tool • Consistent Logging Level Support	Supports fresh installation as well as upgrade from 1.8.x to 1.9.0	Compatible with: • NRF 1.12.0 • UDR 1.12.0 • CNC Policy 1.12.0 • CNDBTier 1.8.7.0 • OSO 1.6.1, 1.7.0 • ASM 1.6.14 • CNE 1.8.3

Table 3-1 (Cont.) Media Pack Contents for Cloud Native Core 2.3.4

Description	Versions	ATS Test Cases Included	Upgrade	Compliance
Oracle Communications Cloud Native Core Binding Support Function (BSF)	1.9.1	Yes **Note:** Not applicable to: • Support for Debug Tool • Consistent Logging Level Support	Supports fresh installation as well as upgrade from 1.8.x to 1.9.1	Compatible with: • NRF 1.12.0 • UDR 1.12.0 • CNC Policy 1.12.0 • CNDBTier 1.8.7.0 • OSO 1.6.1, 1.7.0 • ASM 1.6.14 • CNE 1.8.3
Oracle Communications Cloud Native Core Console (CNCC)	1.7.1	NA	Upgrade from CNCC 1.6.x to 1.7.x is supported	Compatible with: • SCP 1.12.0 • NRF 1.12.0 • UDR 1.12.0 • Policy 1.12.0 • BSF 1.8.0 • CNDBTier 1.8.0 • OSO 1.6.2 • ASM 1.5.7-am3, ASM 1.4.6-am9, 1.6.14-am4 • CNE 1.8.0, CNE 1.7.x, CNE 1.6.0
Oracle Communications Cloud Native Core Console (CNCC)	1.7.0	NA	Upgrade from CNCC 1.6.x to 1.7.0 is supported	Compatible with: • SCP 1.12.0 • NRF 1.12.0 • UDR 1.12.0 • Policy 1.12.0 • BSF 1.8.0 • CNDBTier 1.8.0 • OSO 1.6.2 • ASM 1.5.7-am3, ASM 1.4.6-am9, 1.6.14-am4 • CNE 1.8.0, CNE 1.7.x, CNE 1.6.0
Oracle Communications Cloud Native Core Diameter Routing Agent (CnDRA)	1.6.0	NA	Supports fresh installation only	NA

Table 3-1 (Cont.) Media Pack Contents for Cloud Native Core 2.3.4

Description	Versions	ATS Test Cases Included	Upgrade	Compliance
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 (OCNEF)	1.3.1	No	Supports fresh installation only	Compatible with: • cnDBTier 1.8.7 • OCCNE 1.8.0
Oracle Communications Cloud Native Core Network Repository Function (NRF)	1.12.1	Y	NRF 1.12.1 supports a fresh installation as well as upgrade from 1.11.4 to 1.12.1. For more information on installation or upgrading, see *Oracle Communications Cloud Native Core Network Repository Function Installation and Upgrade Guide.*	Compatible with: • SLF 1.12.0 • cnDBTier 1.8.7 • OSO 1.6.2 • ASM 1.6.14-am.4 • OCCNE 1.8.1 • 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

Table 3-1 (Cont.) Media Pack Contents for Cloud Native Core 2.3.4

Description	Versions	ATS Test Cases Included	Upgrade	Compliance
Oracle Communications Cloud Native Core Network Repository Function (NRF)	1.12.0	Y	NRF 1.12.0 supports a fresh installation as well as upgrade from 1.11.3 to 1.12.0. For more information on installation or upgrading, see *Oracle Communications Cloud Native Core Network Repository Function Installation and Upgrade Guide.*	Compatible with: • SLF 1.12.0 • CNDBTier 1.8.7 (With and Without ASM) • OSO 1.6.2 • ASM 1.6.14-am.4 • OCCNE 1.8.0 • 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
Oracle Communications Cloud Native Core Network Slice Selection Function (NSSF)	1.6.0	Yes	Supports fresh installation only	Compatible with: • CNE 1.8.x • CNDBTier 1.8.x • OSO 1.6.2 • 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 2.3.4

Description	Versions	ATS Test Cases Included	Upgrade	Compliance
Oracle Communications Cloud Native Core Policy (CNC Policy)	1.12.3	Yes **Note:** Not applicable to the following: • Support for Debug Tool • Session Viewer REST API support for GET and DELETE	1.12.3 supports a fresh installation as well as an upgrade from 1.11.x to 1.12.3, based on the selected mode: • **Converged Policy Mode**: In the converged mode, Policy supports only fresh installations. • **PCF Mode**: In PCF mode, the installation or upgrade depends on the CNE version: – With CNE 1.8.0, Policy 1.12.3 supports fresh installation only. – With CNE 1.7.2, upgrade to Policy 1.12.3 from 1.11.x is supported. • **PCRF Mode:** In the PCRF mode, Policy supports only fresh installations. For more information on installation or upgrade, see *Oracle Communications Cloud Native Core Policy Installation and Upgrade Guide*. .	Compatible with: • UDR 1.12.0 • CNDBTier 1.8.7.0 • OSO 1.6.1, 1.7.0 • ASM 1.6.14 • CNE 1.8.3 • CNE 1.7.2 • BSF 1.9.0 • NRF 1.12.0

Table 3-1 (Cont.) Media Pack Contents for Cloud Native Core 2.3.4

Description	Versions	ATS Test Cases Included	Upgrade	Compliance
Oracle Communications Cloud Native Core Policy (CNC Policy)	1.12.2	Yes **Note:** Not applicable to the following: • Support for Debug Tool • Session Viewer REST API support for GET and DELETE	1.12.2 supports a fresh installation as well as an upgrade from 1.11.x to 1.12.2, based on the selected mode: • **Converged Policy Mode**: In the converged mode, Policy supports only fresh installations. • **PCF Mode**: In PCF mode, the installation or upgrade depends on the CNE version: – With CNE 1.8.0, Policy 1.12.2 supports fresh installation only. – With CNE 1.7.2, upgrade to Policy 1.12.2 is supported. For more information on installation or upgrade, see *Oracle Communications Cloud Native Core Policy Installation and Upgrade Guide* .	Compatible with: • UDR 1.12.0 • CNDBTier 1.8.7.0 • OSO 1.6.1, 1.7.0 • ASM 1.6.14 • CNE 1.8.3 • CNE 1.7.2 • BSF 1.9.0 • NRF 1.12.0

Table 3-1 (Cont.) Media Pack Contents for Cloud Native Core 2.3.4

Description	Versions	ATS Test Cases Included	Upgrade	Compliance
Oracle Communications Cloud Native Core Policy (CNC Policy)	1.12.1	Yes **Note:** Not applicable to the following: • Support for Debug Tool • Session Viewer REST API support for GET and DELETE	1.12.1 supports a fresh installation as well as an upgrade from 1.11.x to 1.12.1, based on the selected mode: • **Converged Policy Mode**: In the converged mode, Policy supports only fresh installations. • **PCF Mode**: In PCF mode, the installation or upgrade depends on the CNE version: – With CNE 1.8.0, Policy 1.12.1 supports fresh installation only. – With CNE 1.7.2, upgrade to Policy 1.12.1 is supported. For more information on installation or upgrade, see *Oracle Communications Cloud Native Core Policy Installation and Upgrade Guide* .	Compatible with: • UDR 1.12.0 • CNDBTier 1.8.7.0 • OSO 1.6.1, 1.7.0 • ASM 1.6.14 • CNE 1.8.3 • CNE 1.7.2 • BSF 1.9.0 • NRF 1.12.0

Table 3-1 (Cont.) Media Pack Contents for Cloud Native Core 2.3.4

Description	Versions	ATS Test Cases Included	Upgrade	Compliance
Oracle Communications Cloud Native Core Policy (CNC Policy)	1.12.0	Yes **Note:** Not applicable to the following: • Support for Debug Tool • Session Viewer REST API support for GET and DELETE	1.12.0 supports a fresh installation as well as an upgrade from 1.11.x to 1.12.0, based on the selected mode: • **Converged Policy Mode**: In the converged mode, Policy supports only fresh installations. • **PCF Mode**: In PCF mode, the installation or upgrade depends on the CNE version: – With CNE 1.8.0, Policy 1.12.0 supports fresh installation only. – With CNE 1.7.2, upgrade to Policy 1.12.0 is supported. For more information on installation or upgrade, see *Oracle Communications Cloud Native Core Policy Installation and Upgrade Guide* .	Compatible with: • UDR 1.12.0 • CNDBTier 1.8.7.0 • OSO 1.6.1, 1.7.0 • ASM 1.6.14 • CNE 1.8.3 • CNE 1.7.2 • BSF 1.9.0 • NRF 1.12.0
Oracle Communications Cloud Native Core Service Communication Proxy (SCP)	1.12.1	Yes	1.12.1 supports a fresh installation and an upgrade from 1.12.0 to 1.12.1 For more information about installation and upgrade, see *Oracle Communications Cloud Native Core Service Communication Proxy Installation and Upgrade Guide*	Compatible with: • CNE 1.6.0 • CNE 1.7.0 • CNE 1.8.3 • OSO 1.6 • CnDBTier 1.8.7 • ASM 1.6.14-am4

Table 3-1 (Cont.) Media Pack Contents for Cloud Native Core 2.3.4

Description	Versions	ATS Test Cases Included	Upgrade	Compliance
Oracle Communications Cloud Native Core Service Communication Proxy (SCP)	1.12.0	Yes	Supports fresh installation only	Compatible with: • CNE 1.6.0 • CNE 1.7.0 • CNE 1.8.3 • OSO 1.6 • CnDBTier 1.8.7 • ASM 1.6.14-am4
Oracle Communications Cloud Native Core Security Edge Protection Proxy (SEPP)	1.5.0	Yes	Supports fresh installation only	Compatible with: • cnDBTier 1.8.0.0.3 • OCCNE 1.8.1
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
Oracle Communications Cloud Native Core Unified Data Repository (UDR)	1.12.0	Y	1.12.0 supports a fresh installation as well as upgrade from 1.11.x. For more information on installation or upgrading, see *Cloud Native United Data Repository Installation and Upgrade Guide*	Compatible with: • CNE 1.6.0, 1.7.0 • NRF 1.12.0 • cnDBTier 1.8.0.0.1, 1.8.0.0.3, 1.8.5 • 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 2.3.4.

Common Services Load Lineup for Network Functions

Common Service	BSF	CNC Policy	NRF	NSSF	UDR	SEPP	NEF	CNC Console	SCP
Alternate Route Svc	1.4.2	1.4.2	NA	NA	1.12.2	NA	NA	NA	NA
App-Info	1.12.0	1.12.0	1.12.0	1.12.0	1.12.0	1.12.0	1.12.0	NA	NA

Common Service	BSF	CNC Policy	NRF	NSSF	UDR	SEPP	NEF	CNC Console	SCP
ASM Configuration	1.6.14	1.6.14	1.6.14.am-4	1.6.14.am-4	1.6.14-am4	NA	NA	NA	NA
ATS Framework	NA	NA	NA	NA	1.4.0	NA	NA	NA	1.4.3
Config-Server	1.12.0	1.12.0	NA	1.12.0	1.12.0	1.12.0	1.12.0	NA	NA
Debug-tool	1.0.0	1.0.0	1.0.0	1.0.0	1.10.0	NA	NA	1.0.0	1.0.0
Egress and Ingress Gateway	1.12.2	1.12.2	1.12.2	1.12.2	1.12.2	1.12.2	1.12.2	1.12.2	NA
Helm Test	1.12.0	1.12.0	1.12.0	1.12.0	1.12.0	NA	NA	1.12.0	1.12.0
NRF-Client	1.7.0	1.7.0	NA	1.7.0	NA	1.7.0	1.7.0	NA	NA
Perf-Info	1.12.0	1.12.0	NA	NA	1.12.0	1.12.0	1.12.0	NA	NA

Common Services Load Lineup for ATS

Common Service	UDR ATS
Alternate Route Svc	1.12.2
ASM Configuration	1.12.0
App-Info	NA
ATS Framework	1.4.0
Config-Server	1.12.0
Debug-tool	1.10.0
Egress and Ingress Gateway	1.12.2
Helm Test	1.12.0
NRF-Client	NA
Perf-Info	1.12.0

Security Certification Declaration

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

Table 3-2 Security Certification Declaration

Compliance Test Description	NRF	CNC Policy	BSF	NSSF	UDR	SEPP	CNC Console	NEF	SCP
Systems test on functional and security features	NA (No new security feature)	June 9, 2021	June 9, 2021	NA (No new security feature)	NA (No new security feature)	NA (No new security feature)	NA (No new security feature)	NA (No new security feature)	NA
Regression testing on security configuration	June 5, 2021	June 10, 2021	June 10, 2021	NA	04 Jun 2021	05 Jun 2021 (ATS test cases)	04 Jun 2021	NA	NA
Vulnerability testing	June 5, 2021	June 10, 2021	June 10, 2021	01 Jun 2021	04 Jun 2021	05 Jun 2021	24 May 2021	10 May 2021	23 June 2021
Fuzz testing on external interfaces	12 Jun 2021	June 9, 2021	June 9, 2021	01 Jun 2021	04 Jun 2021	13 May 2021	24 May 2021	10 May 2021	23 June 2021

The following table lists the security tests and the corresponding dates of compliance for ATS.

Table 3-3 Security Certification Declaration

Compliance Test Description	UDR
Systems test on functional and security features	NA (No new security feature)
Regression testing on security configuration	NA
Vulnerability testing	NA
Fuzz testing on external interfaces	NA

Documentation Pack

All documents for Cloud Native Core (CNC) 2.3.4 are available for download on MOS. 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 2.3.4.

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 2.3.4.

CNC Console Resolved Bugs

Table 4-1 CNC Console 1.7.2 Resolved Bugs

Bug Number	Severity	Found in Release	Title
33134335	Minor	1.7.0	CNCC is not supporting ASM with mTLS disabled

Table 4-2 CNC Console 1.7.0 Resolved Bugs

Bug Number	Severity	Found in Release	Title
32918829	Minor	1.6.2	VzW: CNCC 1.6 ServiceDown alert rules do not allow for custom pod name prefixes
32292169	Minor	1.2.0	VZW CNCC: CNCC IAM Pods showing healthy when db is down. No Reading or Liveliness Errors observed
31355530	Minor	1.1.0	CNCC IAM - Unable to remove assigned User Role

BSF Resolved Bugs

Table 4-3 BSF 1.9.0 Resolved Bugs

Bug Number	Severity	Found in Release	Title
32995049	3	1.7.2	bsf-management-service deployment.yaml not checking global.bsfApiRoot for BSF_APIROOT
32995104	3	1.8.1	BSF 1.8.1 performance pod keeps restarting

Table 4-3 (Cont.) BSF 1.9.0 Resolved Bugs

Bug Number	Severity	Found in Release	Title
32995437	3	1.8.1	BSF mgmt unable to find ipv6 binding prefix with 128 length for Rx AAR corresponding prefix length is 64 from SM service
32995469	3	1.7.1	Session viewer doesn't display bindings if SNSSAI is not used

CNC Policy Resolved Bugs

Table 4-4 CNC Policy 1.12.3 Resolved Bugs

Bug Number	Severity	Found In Release	Title
33321419	3	1.12.0	PCF sending NULL smPolicyDecision in audit messages

Table 4-5 CNC Policy 1.12.2 Resolved Bugs

Bug Number	Severity	Found In Release	Title
33208990	3	1.11.3	"attribute in SMF request" block throws unhandled exception when the path in request is not valid
33209010	3	1.11.4	Policy Association table while updating/storing the association fails with error "Data truncation: Data too long for column 'v' at row 1
33209741	3	1.11.0	PRE keeps on polling and retrieving PolicyTable periodically irrespective of any changes done in Policy Table
33209755	3	1.11.4	Null Pointer Exception In PolicyDs when SSV is disabled
33209763	3	1.12.0	Policy custom yaml files are still using the deprecated SCP configuration.

Table 4-6 CNC Policy 1.12.1 Resolved Bugs

Bug Number	Severity	Found In Release	Title
32998157	2	1.11.3	Overload Control: Pending req count is not decreased in IGW
32995443	3	1.11.2	PCF sends PATCH request to UDR even in the absence of policies - not working after fix also
33123449	3	1.12.0	CM GUI : Open Policy Table throws Error when it has Session/PCC Override columns
33123500	3	1.12.0	Diam connector not connecting to new IP of diam-gateway
33123500	3	1.12.0	Diam connector not connecting to new IP of diam-gateway
33123511	3	1.11.2	BSF Selection for IPv6 Prefix not considering the end range
33123529	3	1.11.0	Incorrect QOS rule after PRA change message
33123548	3	1.11.3	SM service unable to trigger "Sent User Service Request" for CHF Info
33123564	3	1.11.3	PCF_SERVICE_DOWN alert does not show all services that are down
33066007	3	1.12.0	send a notification to Syslog blockly is missing in 1.12

Table 4-7 CNC Policy 1.12.0 Resolved Bugs

Bug Number	Severity	Found In Release	Title
32877378	3	1.11.3	DNS Core IP address configuration shall be automated in the DNS stub
32995088	3	1.11.0	UDR and CHF metrics not getting into promethues

Table 4-7 (Cont.) CNC Policy 1.12.0 Resolved Bugs

Bug Number	Severity	Found In Release	Title
32995089	3	1.11.1	SM Create without IP , binding fails even though Session is created
32995091	3	1.11.1	Policy Design: possibility to change the AND/OR block from "horizontal" to "vertical"
32995094	3	1.11.1	PCF includes smPolicySnssaiData= NULL in 'body' written to UDR
32995096	3	1.11.1	PCF doesn't delete Subs State Variables after Session Deleted
32995098	3	1.11.0	PCF generating old diameter routing config file in bulk export
32995101	3	1.11.0	Timer profile not present in bulk policy export
32995012	3	1.11.2	Failed to sent RAR/ASR to AF with different realm
32995022	3	1.11.2	Diameter connection to DAR flash during traffic run
32995030	3	1.11.0	QOS APN-Aggregate-Max-Bitrate-DL/UL AVPs setup
32995031	3	1.11.0	Intermittent VoNR call failures involving PCF. Identified that egress pod is unable to deliver the smpolicycontrol
32995245	3	1.10.3	PCF - No BSF profile selected due to missing bsfInfo but should be optional
32995036	3	1.11.0	Subscriber State Variable Handling Negative Scenario when PATH is configured at Attribute Level
32995041	3	1.11.0	Implement Policy Action to set Charging Server

Table 4-7 (Cont.) CNC Policy 1.12.0 Resolved Bugs

Bug Number	Severity	Found In Release	Title
32995043	3	1.11.0	PCF cannot parse NRF.CHF cfg topic due to unexpected ServiceName value 'nchf-offlineonlycharging'
32995046	3	1.11.2	PA session processing failures - exception: illegal character in the Rx session id URI

Table 4-8 ATS 1.12.0 Resolved Bugs

Bug Number	Severity	Found In Release	Title
32877378	3	1.11.3	DNS Core IP address configuration shall be automated in the DNS stub

NRF Resolved Bugs

Table 4-9 NRF 1.12.1 Resolved Bugs

Bug Number	Severity	Found In Release	Title	Customer Impact
33104786	4	1.10.1	NFDiscover for AMF for AMFSetId in Guami attribute is returning no profiles due to case sensitive match	If Discovery query is sent with AMFSetID of different case then what the producer had used during registration, then the Discovery query will fail, and Consumer NF will not able to discovery the producer even if it is registered. Work Around: Consumer NF needs to send Discovery Query with same case that producer had used during registration

Table 4-9 (Cont.) NRF 1.12.1 Resolved Bugs

Bug Number	Severity	Found In Release	Title	Customer Impact
33108019	4	1.10.1	NFDiscover Query Needs to perform case in-sensitive match for target-nf-fqdn, snssais, requester-snssais, plmn-specific-snssai-list, dnn, tai, amf-region-id, amf-set-id, guami, ue-ipv6-prefix, pgw-ind, pgw-fqdn and upf-iwk-eps-ind	If Discovery query having Hex/Boolean value is sent with different case then what the producer had use during registration, then the Discovery query will fail, and Consumer NF will not able to discovery the producer even if it is registered. Work Around: Consumer NF needs to send Discovery Query with same case that producer had used during registration
33105051	4	1.10.1	Adding of Load using NFUpdate (patch) not working when only NFStatus and Add (load) attribute present in Patch request	NRF will reject the HeartBeat request with load if load is not present during NF Registration. Work Around: NF should always add Load in the NfProfile while registering.
33105412	4	1.12.0	Incorrect values in ATS annotations section for NRF ATS 1.7.0 Guide	ATS Pod will not able to scape metrics from the NRF PODs which will result into test case failure.

Table 4-10 NRF 1.12.0 Resolved Bugs

Bug Number	Severity	Found in Release	Title	Customer Impact
32860876	4	1.10.2	Deleting bulk record from NRF table is creating some time locking issue	DB Replication channel may go down because of which NRF Geo-Redundancy will not work
32973002	4	1.11.2	False metric and log is raised for the response received from SLF	Wrong Metric Value will be pegged
32973008	4	1.7.0	RejectionReason missing in NfAccessToken response metric	When an Access Token is rejected, it will not be known the exact reason for the rejection by looking into metric
32973022	4	1.10.0	Removal of load attribute is setting load attribute in NF Profile to 0. Instead it shall be removed from NF Profile	Removal of load attribute is setting load attribute in NF Profile to 0. Instead it shall be removed from NF Profile

SCP Resolved Bugs

Table 4-11 SCP 1.12.1 Resolved Bugs

Bug Number	Severity	Found in Release	Title
33249040	3	1.11.0	Pod restarts observed with 61.2K TPS when SCP deployed with 31 worker pods.

Table 4-12 SCP 1.12.0 Resolved Bugs

Bug Number	Severity	Found in Release	Title
32792888	2	1.10.2	SCP worker is encoding already encoded query parameters to egress requests URI
33036339	4	1.9.2	Make dimensions consistent for Control plane metrics
32989902	3	1.11.1	URI of notification from scp-w to scp-notification service has an extra '/' appended which is causing 301 error code responses for notifications.
33036348	4	1.11.0	Exception logs for deletion of virtual service during notification processing
32989925	2	1.11.0	Incorrect port picked in URL in case of fqdn only virtual service match
32989894	4	1.11.0	SCP 1.11.1 giving inconclusive value for "request processing time" falling under 2 second bucket
33036414	4	1.11.1	ATS Helm charts update to remove serviceMesh flag
33036425	4	1.11.0	ATS Scale Deployment step fix to wait and retry
33036429	4	1.11.1	ATS retry implementation on failure to fetch Metrics from SUT

SEPP Resolved Bugs

Table 4-13 SEPP 1.5.0 Resolved Bugs

Bug Number	Severity	Found in Release	Title	Customer Impact
32924463	2	1.4.1	n32c handshake failed	If remoteSeppIpAddress is not provided in Roaming profile then n32c fails to initiate handshake. Workaround: Add remote IP address in *remoteSeppIpAddress* parameter when adding roaming profile.
32924486	3	1.4.1	HTTP requests rejected by the SEPP with 503 when using final destination fqdn as authority	When FQDN is set in authority as final destination, n32f message was getting rejected with 503 error.
32924531	4	1.4.1	SEPP config-pre-install pod not connecting to mysql.	*SEPP- config-pre-install* pod is going into error state and not able to connect to the DB. This was due to missing permission in SEPP 1.4.1 installation guide. Workaround: Add the REFERENCES when granting database access permission to user.

UDR Resolved Bugs

Table 4-14 UDR ATS 1.12.1 Resolved Bugs

Bug Number	Severity	Found in Release	Title
CNCES-3022	NA	1.11.0	SLF_Nrf_Client_Scenarios failed-GPSI

Table 4-15 UDR 1.12.0 Resolved Bugs

Bug Number	Severity	Found in Release	Title
31877256	4	1.8.0	ProvGw: GET response sometimes does not have segment1 related data for subscriber does not exist case
32631173	3	1.11.0	udr_rest_request_total not pegged for Unsuppported Media Type messages.

Table 4-15 (Cont.) UDR 1.12.0 Resolved Bugs

Bug Number	Severity	Found in Release	Title
32631219	3	1.11.0	PUT/POST request for policy-data/UDM with empty payloads returns 5xx errors
32631240	3	1.11.0	UDR returns 5012 when vsaLevel set to either dnn or nssai

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.

CNC Console Customer Known Bugs

Table 4-16 CNC Console 1.7.x Customer Known Bugs

Bug Number	Severity	Found in Release	Title	Customer Impact
32291223	Minor	1.5.0	CNCC: CNE Common Services type should be ClusterIP when accessed via CNCC	User will be able to access CNE common services directly using LoadBalancer IP.

CNC Policy Customer Known Bugs

Table 4-17 CNC Policy 1.12.0 Customer Known Bugs

Bug Number	Severity	Found in Release	Title	Customer Impact
32980584	3	1.11.0	LDAP-GW fails to fetch ldap user data after FI and UI.	This issue is seen in converged mode of deployment. For fresh installation, it would work fine but if LDAP-Gateway is installed and upgrade is done - this issue will be observed. Currently, this condition can be recovered on restarting LDAP-Gateway pod.

Table 4-17 (Cont.) CNC Policy 1.12.0 Customer Known Bugs

Bug Number	Severity	Found in Release	Title	Customer Impact
32995076	3	1.11.0	1.12.0 cmgui has configurations related to disabled services in pcrf mode.	Configurations that are not relevant for PCRF mode of deployment may confuse the customers.
32995081	3	1.11.0	Memory leak in diam-connector when diam-gw pod scales	When Diameter Gateway pod scales, Diameter Connector does not release the old connection buffers, which results in memory leak. This condition can be recovered by setting reconnectLimit = 0 in Diameter Connector config map and diam-connector will not reserve any buffers for storing the connection context.
32995443	3	1.11.2	PCF sends PATCH request to UDR even in the absence of policies - not working after fix also	PATCH request is triggered towards Unified Data Repository (UDR) even when remote section is not updated.
32998157	2	1.12.0	Overload Control: Pending req count is not decreased in IGW	This issue may happen under very rapid surges in traffic. Pending Request Count, once increased because of the high surge in traffic, will not reset once overload condition is removed. This will lead to shedding of traffic. This condition can be recovered by restarting Ingress Gateway.

NRF Customer Known Bugs

Table 4-18 NRF 1.11.2 Customer Known Bugs

Bug Number	Severity	Found in Release	Title	Customer Impact
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
32973036	4	1.12.0	More than one allowedXXX attributes are present in NfProfile, then NRF sending Notification if one of allowedXXX check is passing and other(s) are failing	In certain scenarios NF May get notification for a NF even if it is not allowed to access the service of that NF
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.

SEPP Customer Known Bugs

No Customer Known Bugs for SEPP Release 1.5.0.

SCP Customer Known Bugs

No Customer Known Bugs for SCP Release 1.12.0.

UDR Customer Known Bugs

Table 4-19 UDR ATS 1.12.1 Customer Known Bugs

Bug Number	Severity	Found in Release	Title	Customer Impact/WA
32377439	4	1.10.0	De-Registration fails when egressgateway goes down before nrf-client during UDR deletion	No impact

Table 4-19 (Cont.) UDR ATS 1.12.1 Customer Known Bugs

Bug Number	Severity	Found in Release	Title	Customer Impact/WA
32377341	4	1.10.0	Fetch UDM authentication subscription on UDR returns Internal Server Error	Occurs only with cnDBTier. Possible bug on MySQL Cluster
32972133	3	1.12.0	Notify pod not sending notifications everytime to the stub for PATCH of sdmsubscription	Affects only PATCH operations. No workaround
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

Table 4-20 UDR 1.12.0 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 egressgateway goes down before nrf-client during UDR deletion	No impact
32377341	4	1.10.0	Fetch UDM authentication subscription on UDR returns Internal Server Error	Occurs only with cnDBTier. Possible bug on MySQL Cluster

Table 4-20 (Cont.) UDR 1.12.0 Customer Known Bugs

Bug Number	Severity	Found in Release	Title	Customer Impact/WA
32972133	3	1.12.0	Notify pod not sending notifications everytime to the stub for PATCH of sdmsubscription	Affects only PATCH operations. No workaround.