Oracle® Communications

Cloud Native Core Release Notice

Release 2.3.1

F36670-21

October 2021

Oracle Communications Cloud Native Core Release Notice, Release 2.3.1

F36670-21

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:

1. Select **2** for New Service Request.
2. Select **3** for Hardware, Networking and Solaris Operating System Support.
3. Select one of the following options:
    - 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**.

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 in Oracle Communications Cloud Native Core (CNC) network elements for Release 2.3.1.

New and Updated Sections for SCP Release 1.9.3

The following sections are updated for SCP Release 1.9.3:

- Resolved Bug List: Added resolved bugs list
- Media Pack: Added Media pack details

New and Updated Sections for SCP Release 1.9.2

The following sections are updated for SCP Release 1.9.2:

- Service Communication Proxy (SCP): Feature enhancement for SCP 1.9.2 is added.
- Media Pack: Added Media pack details
- Resolved Bug List: Added resolved bugs list

New and Updated Sections for SCP Release 1.9.1.1

The following sections are updated for SCP Release 1.9.1.1:

- Media Pack: Added Media pack details
- Resolved Bug List: Added resolved bugs list

New and Updated Sections for CNC Policy Release 1.9.3

The following sections are updated for CNC Policy Release 1.9.3:

- Media Pack: Added Media pack details
- Resolved Bug List: Added resolved bugs list

New and Updated Sections for SCP Release 1.9.1

The following sections are updated for SCP Release 1.9.1:

- Media Pack: Added Media pack details
- Resolved Bug List: Added resolved bugs list

New and Updated Sections for BSF Release 1.6.0

The following sections are updated for BSF Release 1.6.0:

- Binding Support Function (BSF): Feature enhancement for BSF 1.6.0 is added.
- Media Pack: Added Media pack details
- Resolved Bug List: Added resolved bugs list
- Customer Known Bug List: Added customer known bugs list

New and Updated Sections for SEPP Release 1.4.1

The following sections are updated for SEPP Release 1.4.1:

- Security Edge Proxy Protection (SEPP): Feature enhancement for SEPP 1.4.1 is added.
- Media Pack: Added Media pack details
- Resolved Bug List: Added resolved bugs list
- Customer Known Bug List: Added customer known bugs list

New and Updated Sections for CNE Release 1.7.0

The following sections are updated for CNE Release 1.7.0:

- Cloud Native Environment (CNE): Feature enhancement for CNE 1.7.0 is added.
- Media Pack: Added Media pack details
- Resolved Bug List: Added resolved bugs list
- Customer Known Bug List: Added customer known bugs list

New and Updated Sections for CNCC Release 1.4.0

The following sections are updated for CNCC Release 1.4.0:

- Cloud Native Core Console: Feature enhancement for CNCC 1.4.0 is added.
- Media Pack: Added Media pack details
- Resolved Bug List: Added resolved bugs list
- Customer Known Bug List: Added customer known bugs list

New and Updated Sections for CNC Policy Release 1.9.0 and 1.9.1

The following sections are updated for CNC Policy Release 1.9.0 and 1.9.1:

- Cloud Native Core Policy (CNC Policy): Added feature enhancement for CNC Policy 1.9.0 and 1.9.1
- Media Pack: Added Media pack details
- Resolved Bug List: Added resolved bugs list
- Customer Known Bug List: Added customer known bugs list

New and Updated Sections for CNC Data Collector Tool Release 1.2.0

The following sections are updated for CNC Data Collector Tool Release 1.2.0:

- CNC NF Data Collector: Feature enhancement for CNC Data Collector Tool 1.2.0 is added.

New and Updated Sections for NRF Release 1.9.0

The following sections are updated for NRF Release 1.9.0:

- Network Repository Function (NRF): Feature enhancement for NRF 1.9.0 is added.
- Media Pack: Added Media pack details
- Resolved Bug List: Added resolved bugs list
- Customer Known Bug List: Added customer known bugs list

New and Updated Sections for SCP Release 1.9.0

The following sections are updated for SCP Release 1.9.0:

- Service Communication Proxy (SCP): Feature enhancement for SCP 1.9.0 is added.
- Media Pack: Added Media pack details
- Resolved Bug List: Added resolved bugs list
- Customer Known Bug List: Added customer known bugs list

New and Updated Sections for UDR Release 1.9.0

The following sections are updated for UDR Release 1.9.0:

- Unified Data Repository (UDR): Feature enhancement for UDR 1.9.0 is added.
- Media Pack: Added Media pack details
- Resolved Bug List: Added resolved bugs list
- Customer Known Bug List: Added customer known bugs list

1 Introduction

This Release Notice includes feature descriptions, and media and documentation pack contents. This document includes listings for both the resolved and known bugs for this release. Directions for accessing key Oracles sites and services are explained in MOS. Release Notices are included in the documentation pack made available with every software release.

2
Feature Descriptions

This chapter provides a summary of each feature released in Cloud Native features release 2.3.1.

Binding Support Function (BSF)

Binding Support Function (BSF) 1.6.0 has below enhancements:

- XFCC Header Support: With this enhancement, support for BSF as a producer has been added, to check, if SCP which has sent the HTTP request is the same proxy consumer or client, which is expected to send a HTTP2 request. This is achieved by comparing the FQDN of SCP present in the “x-forwarded-client-cert” (XFCC) of http2 header, with the FQDN of the SCPs configured in BSF. For more information on configurable parameters for XFCC header, see *Oracle Communications Cloud Native Binding Support Function Installation Guide*.
- Aspen Service Mesh Integration: The Aspen Service Mesh integration supports inter-NF communication. The service mesh integration supports the services by deploying a special sidecar proxy in the environment to intercept all network communication between microservices. For more information, see *Oracle Communications Cloud Native Binding Support Function Installation Guide*.
- OSO Integration: BSF supports OSO integration. For more information on integrating BSF with OSO, see *Oracle Communications Cloud Native Binding Support Function Installation Guide*.
- Automated Test Suite for BSF: BSF supports Automated Test Suite. For more information, see *Automated Testing Suite Guide*.
- Enabling GUI and REST to configure Diameter Settings and Peer Nodes: New GUI configurations and REST APIs have been added to configure Diameter Settings and Peer Nodes. For more information on GUI configurations, see *Oracle Communications Cloud Native Binding Support Function User's Guide* and for REST APIs, see *Oracle Communications Cloud Native Binding Support Function REST Specification Guide*.
- CNCC Integration with BSF: BSF is now integrated with CNC Console. For more information on integrating BSF with CNC Console, see *Oracle Communications Cloud Native Binding Support Function User's Guide*.

Cloud Native Environment (CNE)

Cloud Native Environment (CNE) 1.7.0 provides the following major features in this release:

- **CNE Sizing and Performance**: Pre-deployment sizing for OC-CNE virtualized nodes and improved log file management has been introduced in this release. Refer to *OCCNE Installation Guide* for more information.
- **TLS Support for Cross-Site Replication**: DBTier supports manual procedures to configure TLS for cross-site replication using customer-provided keys. Refer to *DBTier User Guide* for more information.

Cloud Native Diameter Routing Agent (CnDRA)

There are no new features or updates implemented in CNC 2.3.1 release.

Cloud Native Core Console

Cloud-Native Core Console (CNCC) 1.4.0 has been updated with the following enhancements::

- Support for Common NF Requirements: Container naming convention is followed in CNCC IAM and CNCC Core helm charts
- Integration with Aspen service mesh 1.5.7
- Integration with CnDBTier for validation of CNCC functionality
- BSF Support - CNCC has enabled BSF GUI, the operator can now perform BSF configurations using CNCC
- Metrics enhancements to define CNCC specific metrics, KPIs and grafana dashboard
- Support OCCNE 1.7.0: Validation of CNCC functionality with OCCNE 1.7.0
- Troubleshooting Tools Container Support: Debug Tool provides third party troubleshooting tools for debugging the runtime issues for lab and production environment. Following are the available tools:
  - tcpdump
  - ip
  - netstat
  - curl
  - ping
  - nmap
  - dig

Refer to *CNCC Installation Guide* for more information.

- Support the latest version of NFs:
  - SCP 1.9.0
  - NRF 1.9.0
  - UDR 1.9.0
  - POLICY 1.9.0
  - BSF 1.6.0

CNC NF Data Collector

Cloud Native Core Network Function Data Collector Tool 1.2.0 has below enhancements:

- Updated content about how to read SCP logs, metrics, and traces inclusion filter keywords. For more information, see the "Appendices" section in the *Cloud Native Core Network Function Data Collector User's Guide*.
- Updated helm 3 commands in the procedures to execute the NF Deployment Data Collector Module and to export and load the NF Logs, Metrics, Traces, and Alerts data. For more information, see the *Cloud Native Core Network Function Data Collector User's Guide*.
- Added a new section to explain the sequence of tasks to execute the NF Logs, Metrics, Traces, Alerts Data Collector Module. For more information, see the "Execute the NF Logs, Metrics, Traces, Alerts Data Collector Module" section in the *Cloud Native Core Network Function Data Collector User's Guide*.
- Added a new section about how to transfer the data collected by Exporter utility. For more information, see the "Transferring the Data Collected by Exporter Utility" section in the *Cloud Native Core Network Function Data Collector User's Guide.*

Cloud Native Core Policy (CNC Policy)

Oracle Communications Cloud Native Core Policy (CNC Policy) 1.9.0 has below enhancements:

- Dynamic variable write on Nudr: This feature enables the operator to save Subscriber State information to UDR from the policy product. The architecture and design is flexible enough to support writing the data to a given data-blob in the UDR. For more information, see *Oracle Communications Cloud Native Core Policy User's Guide* and *Policy Design Guide*.
- NF Name in all metrics: Policy solution now allows you to use NF FQDN as a parameter in all metrics that are reported with NFInstanceId. This helps to understand the reported data better and in a more readable way in the metrics for the operator, achieve consistency across NF for metrics ,KPI names and defining filters. A new tag, nf_name, has been added in the metrics to implement this. For updated CNC Policy Metrics, see Cloud Native Core Policy Metrics in *Oracle Communications Cloud Native Core Policy User's Guide*.
- Phase- 2 of "Retry On Alternate SCP, Producer and Consumer": Session Retry feature introduced in Release 1.8.0 has been enhanced in this release to include retry on NRF, AMF, AF/NEF and not selecting the producer/consumer when retry after header is present in the previous response. To implement this enhancement, new parameters, “Retry Profile for Initial Messages” and “Retry Profile for Subsequent Messages” have been added for SM service and User Connector service. For more information on these parameters, see *Oracle Communications Cloud Native Core Policy User's Guide*.
- Manually Delete Session from Policy: Policy solution enhances its existing query service to allow operators to delete session(s) for a subscriber manually using the Session Viewer screen on CNC Console. For more information, see *Oracle Communications Cloud Native Core Policy User's Guide.*
- Consistent Logging level configuration: Policy solution now supports configuration of consistent log level for different Policy services through Cloud Native Core Console and REST API. For more information about configuring through CNC console, see Configuring Consistent Level Configuration section in *Oracle Communications Cloud Native Core Policy User's Guide*. For more information, about configuring through REST API, see *Oracle Communications Cloud Native Core Policy REST API Specification* document.

- Asynchronized access to Nchf: Policy solution now supports asynchronized access of subscriber related information from data sources like CHF. For more information, see Asynchronized access to Nchf section in *Oracle Communications Cloud Native Core Policy User's Guide*.
- Integrated with cnDBTier: Policy solution is now integrated with cnDBTier 1.6.0.0.1 and supports OSO 1.6.1 and 1.7.0 for common operation services on a previously installed Kubernetes cluster. For more information, see *Oracle Communications Cloud Native Core Policy Installation Guide*.
- Helm Test Support: Policy solution is now integrated with helm test application. To implement this, a new docker image, oc-helm-test has been added. For more information, see *Oracle Communications Cloud Native Core Policy Installation Guide*.

Inter-Working Function (IWF)

There are no new features or updates implemented in CNC 2.3.1 release.

Service Communication Proxy (SCP)

SCP 1.9.2 has been updated with the following enhancements:

- Preventive Audit before Last NF Deletion: SCP can control NRF failure scenarios in the network by performing the preventive audit. This audit is performed with all the configured regional NRFs before removing the last NF instance of a particular NF type. If any NRF returns the success discovery response with NF profiles, SCP creates the routing rules based on the discovery response. SCP raises an alert to notify operators about such NRF failure scenarios. This feature uses the `preventiveAuditOnLastNFInstanceDeletion` flag defined under the **global** parameter section in the **ocscp_custom_values.yaml** file. For information about enabling and disabling this flag, see the *Oracle Communications Cloud Native Core Service Communication Proxy (SCP) Installation Guide*.
- Audit enhancement to ignore serving scope from NF Profile Hash calculation: SCP supports including or excluding serving scope in NF profile hash calculation. This feature uses the `ignoreServingScopeforNFProfileHash` parameter defined under the **global** parameter section in the **ocscp_custom_values.yaml** file. For information about enabling and disabling this flag, see the *Oracle Communications Cloud Native Core Service Communication Proxy (SCP) Installation Guide*.

SCP 1.9.0 has been updated with the following enhancement:

- Inter-SCP Routing between regions of the same PLMN: SCP learns the network topology by interacting with NRFs in different regions and also discovers other SCPs in the network. Consumer's SCP in a region is aware of the producer's SCP in all other regions to enable routing towards the producer NF instances in other regions. Refer to *SCP Installation Guide* for more information.
- SCP Integration with cnDBTier: Supports cnDBTier in a containerized Cloud Native Environment. Refer to *SCP Installation Guide* and *cnDBTier Installation Guide* for more information.
- Helm test Support: Helm Test feature validates successful installation of SCP and determine if the NF is ready to take traffic. Refer to *SCP Installation Guide* for more information.

- Support for LifeCycleManagement of the CRDs using crdLCMViaHelm flag has been introduced in this release. Refer to *SCP User's Guide* for more information.
- Metrics Enhancements: Refer to SCP User's Guide for more information. The *What's New in This Guide* section of *SCP User's Guide* mentions all the updated list of metrics.
- Support for Debug Tool (per pod): Debug Tool provides third party troubleshooting tools for debugging the runtime issues for lab and production environment. Following are the available tools:
  - tcpdump
  - ip
  - netstat
  - jq
  - curl
  - ping
  - nmap
  - dig

  Refer to *SCP Installation Guide* for more information.

Security Edge Proxy Protection (SEPP)

Security Edge Proxy Protection (SEPP) 1.4.0 provides the following major feature in CNC 2.3.1 release.

- Support for N32 Interface with TLS protection mode
  - N32-C Interface support
  - N32-F Interface support
  - 3GPP-Target-SBI-API-Root header support
- API for Roaming Partner Profile Configuration
- NRF Registration Support
- Logging, Alerts and Metrics support: Metrics and Alerts support has been updated. For more information on the metric details, see Cloud Native *Security Edge Proxy Protection (SEPP) User's Guide*.

Network Exposure Function (NEF)

There are no new features or updates implemented in CNC 2.3.1 release.

Network Repository Function (NRF)

OCNRF 1.9.0 has been updated with the following enhancements:

- Integration with CnDBTier: This enables operator to use CnDBTier in OCNRF. Refer to *OCNRF Installation and Upgrade Guide* for more information.
- In Service Software Upgrade support (ISSU) for Geo Redundant NRF: This enables the operator to perform ISSU from OCNRF 1.9.0 onwards for both standalone and Geo-

Redundant OCNRF deployment. Refer to *OCNRF Installation and Upgrade Guide* for more information.

- Support for Helm Test: This enables the operator to validate the OCNRF deployment post Install/Upgrade. Refer to *OCNRF Installation and Upgrade Guide* for more information.
- Redesign of NRF Configuration APIs: With this feature OCNRF has broken one big configuration API to small logically grouped APIs. This give the flexibility to the operator to read/configure only a small set of configuration. This also significantly enhanced the usability of OCNRF CNCC GUI. Refer to *OCNRF User's Guide* for more information.
- Support for consistent logging fields across NRF Micro-Services: OCNRF now supports a consistent common set of logging fields across all micro-service logs. Refer to *OCNRF User's Guide* for more information.
- Support for NF Consumer FQDN in NRF Metrics: NF Consumer FQDN in NRF Metrics that are currently reported with NFInstanceId. Refer to *OCNRF User's Guide* for more information.
- SLF Feature Enhancement: Following SLF feature enhancements has been introduced in this release:
  - Support to avoid SLF query if GroupId is already present in the discovery request
  - Support for returning successful discovery response if Subscriber is not provisioned in SLF

  Refer to *OCNRF User's Guide* for more information.
- Troubleshooting Tools Container Support: Debug Tool provides third party troubleshooting tools for debugging the runtime issues for lab and production environment. Following are the available tools:
  - tcpdump
  - ip
  - netstat
  - jq
  - curl
  - ping
  - nmap
  - dig

  Refer to *OCNRF Installation Guide* for more information.

Network Slice Selection Function (NSSF)

There are no new features or updates implemented in CNC 2.3.1 release.

Unified Data Management (UDM)

There are no new features or updates implemented in CNC 2.3.1 release.

Unified Data Repository (UDR)

UDR 1.9.0 has been updated with the following enhancements:

- SOAP/XML support using ProvGw for Converged Policy DB Solution: For information on this feature, refer to *Provisioning Gateway Interface Specification Guide*.
- On-demand migration of 4G policy data to 5G UDR: Using this feature, 4G subscribers can be migrated to 5G UDR on demand. For information on this feature, refer to *UDR User's Guide*.
- Disaster Recovery Procedures - DB-Backup and Restore: UDR data backup and restore procedures are covered in *Disaster Recovery Guide*.
- Integrated with cnDBTier: This enables operator to use CnDBTier in UDR. For more information, refer to *UDR Installation and Upgrade Guide*.
- Integrated with debug tool - Introduction to debug tool and its usage to UDR operators is covered in the *UDR Installation and Upgrade Guide*.

3
Media and Documentation

Oracle Communications software is available for electronic download on the Oracle Software Delivery Cloud (OSDC). Documentation is delivered electronically on the My Oracle Support (MOS). Both the software Media Pack and Documentation Pack are listed in this chapter.

Media Pack

This section lists the media package for Cloud Native Core 2.3.1. For downloading the package, refer to MOS.

> **Note:**
>
> This list 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 2.3.1

Description	Versions	ATS Test Cases Included	Upgrade	Compliance
Oracle Communications Cloud Native Core Automated Testing Suite (ATS)	1.4.0	NA	Supports fresh installation only	Compatible with CNE 1.6.0
Oracle Communications Cloud Native Core Binding Support Function (BSF)	1.6.0	Yes **Note**: Not applicable to: • Aspen Service Mesh Integration • BSF OSO Integration • Kubernetes annotations and label support • Enabling GUI and REST to configure Diameter Settings and Peer Nodes • CNCC Integration with BSF	Supports fresh installation only	Compatible with NRF 1.8.0 and UDR 1.8.0, and CNC Policy 1.8.0
Oracle Communications Cloud Native Core Console (CNCC)	1.4.0	NA	Supports fresh installation only	Compatible with SCP 1.9.0, NRF 1.9.0, UDR 1.9.0, POLICY 1.9.0, BSF 1.6.0, and OCCNE 1.6.0 / 1.7.0

Table 3-1 (Cont.) Media Pack Contents for Cloud Native Core 2.3.1

Description	Versions	ATS Test Cases Included	Upgrade	Compliance
Oracle Communications Cloud Native Core Cloud Native Environment (CNE)	1.7.0	NA	Upgrade supported from OCCNE 1.5.0 to OCCNE 1.6.0. For more information, refer the *CNE Upgrade Guide*.	NA
Oracle Communications Cloud Native Core Policy (CNC Policy)	1.9.3	Yes	CNC Policy 1.9.3 supports upgrade from CNC Policy 1.9.x. For more information on installation/ upgrading, see *Oracle Communications Cloud Native Core Policy Installation and Upgrade Guide*.	Compatible with OCCNE 1.6.0, OSO 1.6.0, BSF 1.6.0, NRF 1.9.0, and UDR 1.9.0.
Oracle Communications Cloud Native Core Policy (CNC Policy)	1.9.2	Yes	CNC Policy 1.9.2 supports upgrade from CNC Policy 1.9.x. For more information on installation/ upgrading, see *Oracle Communications Cloud Native Core Policy Installation and Upgrade Guide*.	Compatible with OCCNE 1.6.0, OSO 1.6.0, BSF 1.6.0, NRF 1.9.0, and UDR 1.9.0.
Oracle Communications Cloud Native Core Policy (CNC Policy)	1.9.1	Yes	CNC Policy 1.9.1 supports upgrade from CNC Policy 1.9.0. For more information on installation/ upgrading, see *Oracle Communications Cloud Native Core Policy Installation and Upgrade Guide*.	Compatible with OCCNE 1.6.0, OSO 1.6.0, BSF 1.6.0, NRF 1.9.0, and UDR 1.9.0.

Table 3-1 (Cont.) Media Pack Contents for Cloud Native Core 2.3.1

Description	Versions	ATS Test Cases Included	Upgrade	Compliance
Oracle Communications Cloud Native Core Policy (CNC Policy)	1.9.0	Yes **Note**: Not applicable to: • ContainerDB Integration • Diameter Gateway scaling continuation • Helm Test Support	CNC Policy 1.9.0 supports a fresh installation as well as upgrade from CNC Policy 1.8.x to CNC Policy 1.9.0. For more information on installation/ upgrading, see *Oracle Communications Cloud Native Core Policy Installation and Upgrade Guide*.	Compatible with OCCNE 1.6.0, OSO 1.6.0, BSF 1.6.0, NRF 1.9.0, and UDR 1.9.0.
Oracle Communications Cloud Native Core Diameter Routing Agent (CnDRA)	1.6.0	NA	Supports fresh installation only	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)	1.2.0	NA	Supports fresh installation only	NA
Oracle Communications Cloud Native Core Network Repository Function (NRF)	1.9.0	Yes **Note**: Not applicable to: • Upgrade enhancement of Geo-Redundancy • NRF Client enhancement	Supports fresh installation only	Compatible with network functions which are compliant with 3GPP Release 29.510 v15.5 (September 2019)
Oracle Communications Cloud Native Core Network Slice Selection Function (NSSF)	1.4.0	NA	Supports fresh installation only	Compatible with any NRF, AMF that supports 3GPP Release 15.5 Specs

Table 3-1 (Cont.) Media Pack Contents for Cloud Native Core 2.3.1

Description	Versions	ATS Test Cases Included	Upgrade	Compliance
Oracle Communications Cloud Native Core Security Edge Protection Policy (SEPP)	1.4.1	Yes	Supports fresh installation as well as upgrade from 1.4.0 to 1.4.1. For more information on installation or upgrading, see Oracle Communications Cloud Native Core Security Edge Protection Proxy (SEPP) Installation Guide.	Compatible with CNE 1.6.0
Oracle Communications Cloud Native Core Service Communication Proxy (SCP)	1.9.3	Yes	Supports fresh installation only	Compatible with CNE 1.5.0, CNE 1.6.0, CNE 1.7.0, OSO 1.6.1, CnDBTier 1.6.x, CnDBTier 1.8.0 (without ASM) and ASM 1.4.6-am9
Oracle Communications Cloud Native Core Service Communication Proxy (SCP)	1.9.2	Yes	Supports fresh installation only	Compatible with CNE 1.5.0, CNE 1.6.0, CNE 1.7.0, OSO 1.6.1, CnDBTier 1.6.x, CnDBTier 1.8.0 (without ASM) and ASM 1.4.6-am9
Oracle Communications Cloud Native Core Service Communication Proxy (SCP)	1.9.1.1	Yes	Supports fresh installation only	Compatible with CNE 1.5.0, CNE 1.6.0, CNE 1.7.0, OSO 1.6.1, CnDBTier 1.6.x, CnDBTier 1.8.0 (without ASM) and ASM 1.4.6-am9
Oracle Communications Cloud Native Core Service Communication Proxy (SCP)	1.9.1	Yes	Supports fresh installation only	Compatible with CNE 1.5.0, CNE 1.6.0, CNE 1.7.0, OSO 1.6.1, CnDBTier 1.6.x, CnDBTier 1.8.0 (without ASM) and ASM 1.4.6-am9

Table 3-1 (Cont.) Media Pack Contents for Cloud Native Core 2.3.1

Description	Versions	ATS Test Cases Included	Upgrade	Compliance
Oracle Communications Cloud Native Core Service Communication Proxy (SCP)	1.9.0	Yes	Supports fresh installation only	Compatible with CNE 1.5.0, CNE 1.6.0, CNE 1.7.0, OSO 1.6.1, CnDBTier 1.6.x, CnDBTier 1.8.0 (without ASM) and ASM 1.4.6-am9
Oracle Communications Cloud Native Core Unified Data Repository (UDR)	1.9.0	Yes **Note**: Not applicable to: • DB Backup • Restore Testing	Supports fresh installation only	Compatible with CNE 1.5.0, CNE 1.6.0, CNE 1.7.0, NRF 1.7.0, NRF 1.8.0, and NRF 1.9.0
Oracle Communications Cloud Native Core Unified Data Management (UDM)	1.1.0	NA	Supports fresh installation only	NA

Documentation Pack

All documents are available for download from the MOS site.

4
Resolved and Known Bugs

This chapter lists the resolved and known bugs for Cloud Native Core release 2.3.1.

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 2.3.1.

Table 4-1 BSF 1.6.0 Resolved Bugs

Bug Number	Severity	Found in Release	Title
31973019	3	1.5.0	S-NSSAI shall be Optional parameter in bsf discovery
32098522	3	1.5.0	BSF:1.4: pcfbnding discovery failed when we added s-nssai in the query parameters.
32098534	3	1.5.0	BSF:1.5: Session Viewer to support querying session information based on IPv6 in BSF

Table 4-2 CNE 1.7.0 Resolved Bugs

Bug Number	Severity	Found in Release	Title
OCCNE-3467	2	1.6.0	occne/db_backup_svc:1.7.0 docker image is missing in the occne deliverable
OCCNE-3466	2	1.6.0	MySQL Cluster ERROR: Failed to allocate nodeid... No configured host found
OCCNE-3411	2	1.6.0	1.7.0-rc.7 BM upgrade identified issues
OCCNE-3338	2	1.6.0	Uplift Prometheus from v2.19.0 to v2.19.3
OCCNE-3385	2	1.6.0	1.7 vcne metallb deployment fails because of missing scripts and templates on lbvm
OCCNE-3321	2	1.6.0	Upgrade Vcne 1.7- Drain node task fails when pods on worker nodes take more than 3 minutes to terminate
OCCNE-3302	2	1.6.0	Grafana is not configured properly for accessing Prometheus as data source
OCCNE-3278	2	1.7.0	Bare Metal installation error in provision dbtier_bck_part role

Table 4-2 (Cont.) CNE 1.7.0 Resolved Bugs

Bug Number	Severity	Found in Release	Title
OCCNE-3274	2	1.7.0	Upgrade 1.6 -> 1.7 failed for metallb task when upgrade octavia deployment.
OCCNE-3358	3	1.7.0	1.7 Install/Upgrade- Node exporter crashes/ restarts because of lack of resources

Table 4-3 CNC Console 1.4.0 Resolved Bugs

Bug Number	Severity	Found in Release	Title
31958022	Minor	1.3.0	CNCC Core cmservice does not add helm/deployment name
31958056	Minor	1.3.0	CNCC cmservice pod does not come up in Webscale/ASM platform
32061426	Minor	1.3.0	CNCC Helm Test pod does not have Annotation Mustache code
32061435	Minor	1.3.0	CNCC Helm test failing - CPU/Memory requests/limits not specified
32089275	Minor	1.3.0	Install Doc issue page 3.3 Version 1.3

Table 4-4 CNC Policy 1.9.3 Resolved Bugs

Bug Number	Severity	Found in Release	Title
32505516	3	1.9.0	PCF 1.9 egress gateway shows constant oauth errors with oauth disabled.

Table 4-5 CNC Policy 1.9.2 Resolved Bugs

Bug Number	Severity	Found in Release	Title
32427167	3	1.9.0	Policy 1.9.0- pre-install pods cannot create db connection with ASM istio-proxy (possible race condition)

Table 4-6 CNC Policy 1.9.1 Resolved Bugs

Bug Number	Severity	Found in Release	Title
32150019	3	1.9.0	In the POST subscribe message to UDR, 'monitoredResourceUri' in 'PolicyDataSubscription' is not correct (when behind egress gw)
32150047	3	1.9.0	On AM-DELETE, udr-connector is responding with 500 INTERNAL_SERVER_ERROR

Table 4-6 (Cont.) CNC Policy 1.9.1 Resolved Bugs

Bug Number	Severity	Found in Release	Title
32263920	3	1.9.0	UDR Connector throwing "Error : Could NOT find any NFProfile" intermittently on UDR GET Request & returning to PDS with 500 Internal Server Error
32263949	3	1.9.0	PolicyDS - Support for Configurable Http2 Client Connections
32263962	3	1.8.0	ndbcluster produces error Got error 631 when reading table './ocpm_config_server_180/configuration_item' and PCF produces error calls
32264710	3	1.9.0	1.8.2 to 1.8.3 Upgrade --> Rollback --> re-upgrade issue/failure This issue is there in 1.9.0 release as well and fixed in 1.9.1 to safeguard any further upgrades
32264711	3	1.9.0	Performance degradation observed in NRF-client 1.4.1 with PCF
32264748	3	1.9.0	Missing QOS in the N7 notify after receive prevous N7 notify with 400 BAD_REQUEST and ASR/STR
32264778	3	1.9.0	PCF 1.9.0 am-service/ue-service update notify issue
32264787	3	1.9.0	Async CHF workflow update to be future proof
32264816	3	1.9.0	CHF record not deleted in PDS for Delete SMPolicyAssociation

Table 4-7 CNC Policy 1.9.0 Resolved Bugs

Bug Number	Severity	Found in Release	Title
32146813	2	1.8.3	PCF does not send SuppFeatures IE for PRA in SM Policy Association Response
31972768	3	1.8.0	Config Client Connection to Config Server hangs when DB issues are encountered
31895171	3	1.8.0	SM & User-service are not able to connect to alternate service with default 8000 port(unified port)
31898693	3	1.8.0	On loss of connectivity with OCS, Diam Gateway failed to reconnect to OCS
32146883	3	1.8.1	OSO Prometheus shows PCF pods down
32146966	3	1.8.1	ATS - DNS Pod configuration requires each time, when DNS pod gets restarted

Table 4-8 NRF 1.9.0 Resolved Bugs

Bug Number	Severity	Found in Release	Title
32135588	3	1.8.0	PI-D NRF ATS Forwarding test cases (VIA header) issue
32127690	3	1.5.1	When SLF feature is Disabled and SupportedNfTypeList is populated with Target NFType then SUPI from discovery query is getting ignored
32127687	4	1.5.0	Supported NF type list for SLF query is missing in NRF User Guide
32127686	4	1.8.0	CSAR Package updates required for Automation
32127679	4	1.8.0	Incorrect metrics reference in KPIs section of NRF User Guide
31866858	4	1.7.0	replicationstatus alert should not be raised when Geo-Redundancy feature is disabled
31866838	4	1.7.2	Propagating Jaeger Headers for Forwarding/SLF requests
31866770	4	1.7.2	NRF service containers should not send HTTPs request to Sidecar container
32140518	4	1.8.0	Limit NRF-ATS RBAC Verbs and Resource list

Table 4-9 SEPP 1.4.1 Resolved Bugs

Bug Number	Severity	Found in Release	Title
31971775	2	1.4.0	pSEPP incorrectly update path in request URI
32098361	4	1.4.0	n32f requests metrics missing peer fqdn and domain

Table 4-10 SCP 1.9.3 Resolved Bugs

Bug Number	Severity	Found in Release	Title
33429818	2	1.9.2	Addition/deletion of service in NF profile results in incorrect destination rules on SCP
33429831	3	1.9.2	Timestamp format update for SCP control plane services logs

Table 4-11 SCP 1.9.2 Resolved Bugs

Bug Number	Severity	Found in Release	Title
32653951	2	1.9.1	AuditMaster thread is getting killed during DB exception

Table 4-11 (Cont.) SCP 1.9.2 Resolved Bugs

Bug Number	Severity	Found in Release	Title
32699283	3	1.9.1	Handle Concurrent Modification Exception
32699327	4	1.9.1	Different log level shows for the same log

Table 4-12 SCP 1.9.1.1 Resolved Bugs

Bug Number	Severity	Found in Release	Title
32553200	2	1.9.1	IGW gets into a failed state after heavy traffic before hitting CPU threshold for HPA
32553188	2	1.9.1	Issues with Ingress Gateway 1.10 with timeouts & added latency

Table 4-13 SCP 1.9.1 Resolved Bugs

Bug Number	Severity	Found in Release	Title
32358097	3	1.7.4.1, 1.8.0	Topology source information is not retained after configuration pod restart
32215993	3	1.7.4.1	Ingress Gateway memory usage alarm addition: • SCPIngressGatewayPodAboveMinorMemoryUsage • SCPIngressGatewayPodAboveMajorMemoryUsage • SCPIngressGatewayPodAboveCriticalMemoryUsage
32216030	2	1.7.4.1	Intermittent 503 Error by Ingress gateway due to out of memory
32359780	4	1.8.0	Include Alerts and Dashboard files to CSAR
32359767	4	1.8.0	Update the vnfd.yaml file for SCP to not put NF name - in the product_name value

Table 4-14 SCP 1.9.0 Resolved Bugs

Bug Number	Severity	Found in Release	Title
32134953	3	1.7.3	Modify SCP Role definition to remove wild card verbs (*)

Table 4-14 (Cont.) SCP 1.9.0 Resolved Bugs

Bug Number	Severity	Found in Release	Title
32134966	3	1.7.4	SCP Metrics dashboard needs to be corrected from the metric "ocscp_http_0_0_0_80_downstream_cx_active" to the metric "ocscp_http_downstream_cx_active"
32134973	3	1.7.3	Remove CRD creation as part of SCP installation
32134976	3	1.7.4	Success and Failure metric in Audit module
32135488	3	1.7.3	Exception due to NotEmpty constraint on PlmnId in taiRange class
32135496	3	1.7.3	Duplicate entries with empty SCP identifier is created in NRF_NF_DETAILS table after configuration pod restart
32135505	3	1.7.4	Security context addition to helm charts to enable custom user id for SCP containers

Note:

SCP 1.9.0 also includes bug fixes from SCP 1.7.5 patch release.

Table 4-15 UDR 1.9.0 Resolved Bugs

Bug Number	Severity	Found in Release	Title
31889017	3	1.8.0	Issues observed on ProvGw on ASM machine

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.

Table 4-16 BSF 1.6.0 Customer Known Bugs

Bug Number	Severity	Found in Release	Title	Customer Impact
32098543	3	1.6.0	Seagull process are not cleaned and ended up as defunct process	During ATS execution 1 defunct process will be created after the ATS run is complete. This defunct process will not utilize the RAM or CPU so it will not be an impact on the resources. But process Id will be utilized that can cause impact in long run.
32098560	3	1.6.0	ATS documentation in Chrome Browser not getting displayed properly	ATS documentation is not rendering correctly in chrome. The same is opening up correctly in Firefox and IE.
32098550	3	1.5.0	BSF responds with UNKNOWN_SESSION_ID when binding is not found	AAA is received with error UNKNOWN_SESSION_ID from BSF Connector instead of IP-CAN_SESSION_NOT_AVAILABLE.

Table 4-17 CNE 1.7.0 Customer Known Bugs

Bug Number	Severity	Found in Release	Title
30756164	3	1.3.2	OCCNE 1.3 Bare Metal Installation Failure -- Replication IP not configured on Sql Nodes during Db-Tier installation
30756201	4	1.3.2	OCCNE 1.3 Bare Metal Installation Failure -- Pipeline.sh is not documented. Must be continually restart on error.
30371715	4	1.3.2	OCCNE 1.2.0 Installation Guide Does Not Provide Guidance on Firmware Version

Table 4-18 CNC Console 1.4.0 Customer Known Bugs

Bug Number	Severity	Found in Release	Title	Customer Impact
31355530	4	1.1.0	CNCC IAM - Unable to remove assigned User Role	User will be able to add roles but user will not be able to remove the assigned roles.

Table 4-19 CNC Policy 1.9.0 Customer Known Bugs

Bug Number	Severity	Found in Release	Title	Customer Impact
32146869	2	1.8.0	High Latency & timeout observed when Ingress TPS is > 750 - Single POD	Observed performance latency when running beyond750 TPS per pod when PCF is deployed with Aspen Service Mesh
32146896	2	1.8.0	ndbcluster produces error Got error 631 when reading table	Getting temporary error 631 'Scan take over error, restart scan transaction' from NDBCLUSTER while accessing DB. There is no direct impact but this may impact the high performance run.
32146961	3	1.9.0	PCF:1.9.0:PDS timeout happens for first call (ATS case is failing)	After the restart of the PDS service first call will fail.
32147046	3	1.9.0	Notification URI for nCHF is not valid in nCHF Connector Pod Trace	No Impact, log traces will have the wrong notification URI which may be confusing.
32147073	3	1.9.0	PDS Project PRE Evaluation Failing with "Error 6/ invalid_frame_length"	User will not be able to control the call flow of PDS Project through policies. Call flow can be controlled using the Work Flows.
32150019	3	1.9.0	In the POST subscribe message to UDR, 'monitoredResourceUri' in 'PolicyDataSubscription' is not correct (when behind egress gw)	In the POST subscribe message to UDR, 'monitoredResourceUri' in 'PolicyDataSubscription' is not correct (when behind egress gw)
32150047	3	1.9.0	On AM-DELETE, udr-connector is responding with 500 INTERNAL_SERVER_ERROR	On AM-DELETE, udr-connector is responding with 500 INTERNAL_SERVER_ERROR

Table 4-20 NRF 1.9.0 Customer Known Bugs

Bug Number	Severity	Found in Release	Title	Customer Impact
32127692	3	1.1.0	NRF not accepting Discovery Query with SUPI, if the value is not having "imsi-" or "nai-" prefix	Discovery query with format other than "imsi-" or "nai-" will be rejected as back request by NRF
32127694	4	1.1.0	tacRangeList attribute in TaiRange is mandatory, if it is missed OCNRF not reporting bad request rather 500 response is returned	Incorrect error code will be sent to the consumer NF by which it will never know that the request message is having syntax issue.

SEPP 1.4.1 Customer Known Bugs

Note:

Security Edge Protection Proxy (SEPP) 1.4.1 has no customer known bugs.

Table 4-21 SCP 1.9.0 Customer Known Bugs

Bug Number	Severity	Found in Release	Title	Customer Impact
30731782	4	1.2	Limit of VS size is limited to 1 Mb by etcd/k8s.	Impacts only if there are 100s of NFs with many service instances/NF.
30731844	4	1.3	Processing time of NRF notifications increases if more profiles (>10) with more many service instances (more than 10/ profile)are registered. increase observed is 2-3 seconds more than previous registered in case of new registration. Updates also increases with more number of registered profiles.	There may be delay in rule creation if profiles are large in numbers.
30731829	4	1.4	SCPC-Pilot is taking high CPU while applying updates if number of equivalent profiles/ ServiceInstances are exceeding 100	There may be delay in rule creation if profiles are large in numbers which can cause some call failures.

Table 4-22 UDR 1.9.0 Customer Known Bugs

Bug Number	Severity	Found in Release	Title	Customer Impact
30774755	3	1.4.0	Headers for few resources are not implemented as per spec 29505-v15.4.0	No Impact
31889017	3	1.9.0	On demand migration issue for PATCH operation on UDR Rel. 1.8.4	No impact. This is a negative scenario
32122140	3	1.9.0	Subscriber Entity field issues on ProvGw from SOAP/XML	No impact. The error codes needs changes.
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.
31877256	4	1.8.0	ProvGw: GET response sometimes does not have segment1 related data for subscriber does not exist case	No impact. It is intermittent issue.