Oracle® Communications
Cloud Native Core Release Notice

Release 2.2.0

F31856-02

June 2020

ORACLE®

Oracle Communications Cloud Native Core Release Notice, Release 2.2.0

F31856-02

Contents

List of Tables

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 2.2.0.

New and Updated Features in Network Repository Function (NRF) Release 1.6.1

The following sections are updated for NRF Release 1.6.1:

- Media Pack: NRF 1.6.1 media pack information is added.
- Resolved Bug List: Bugs fixed in NRF 1.6.1 are updated.
- Customer Known Bug List: Bugs that are known in NRF 1.6.1 are updated.

New and Updated Features in CNC Release 2.2.0

The following sections are updated for CNC Release 2.2.0:

- Feature Descriptions: The feature specific enhancements implemented in each Network Functions (NFs) are explained in this section.
- Media and Documentation : The media and documentation details are mentioned under this section.
- Resolved and Known Bugs: The bugs that are resolved amd known are listed under this section.

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 also identified in the Oracle References and Services chapter. 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 2.2.0.

Automated Testing Suite (ATS)

ATS 1.1.0 has been updated with the following enhancements:

- Provides an end-to-end solution to the customers for testing Oracle Communications 5G-NFs.
- Docker image of HTTP Server simulator
- Helm chart to deploy the ATS (delivered as a tar file)
- Enables all the NF teams with the basic environment, framework and a GUI (Jenkins) to execute all the functional test cases.

Cloud Native Environment (OCCNE)

There are no new features/updates implemented in CNC 2.2.0 release.

Cloud Native Core Console (CNCC)

Cloud Native Core Console (CNCC) 1.1.0 has been updated with the following enhancements:

- HTTPs/Security Support
- Support of UDR GUI: Following UDR Provisioning Screens are supported:
  - Profile Data
  - PCF
  - UDM
  - SLF
  - Schema Management
- Support of PCRF GUI: Following menu items will be enabled as part of PCRF:
  - PCRF
  - Policy Management
  - Policy Common Configurations
- Session Management: Idle timeout is helm configurable.

Cloud Native Diameter Routing Agent (CnDRA)

CnDRA 1.6.0 has been updated with the following enhancements:

- 1000 connections per pod and 12K connection per CNDRA deployment support.
- Supports Diameter Redirect.
- Supports Mediation Feature.
- address-pool configuration per DRA deployment.
- Automated Testing Suite (ATS).

Binding Support Function (BSF)

There are no new features/updates implemented in CNC 2.2.0 release.

Inter-Working Function (IWF)

There are no new features/updates implemented in CNC 2.2.0 release.

Network Exposure Function (NEF)

There are no new features/updates implemented in CNC 2.2.0 release.

Network Repository Function (NRF)

OCNRF 1.6.0 has been updated with the following enhancement:

- Support for NRF Service Operation Forwarding.
- Support of NRF Alert Rules and SNMP Traps.

Network Slice Selection Function (NSSF)

NSSF version 1.3.0 has been updated with the following enhancements:

- Support for HTTP PATCH method for NS-Availability Update.
- Support for HTTPS (TLSV1.2, Mutual)
- Support for OAuth
- Support Rate limiting

Policy Control Function (PCF)

PCF 1.6.1 has been updated with the following enhancement:

- Supports LDAP
- Supports EPS Fallback
- Supports Policy and Session Variables

- Supports for Policy Table
- Subscriber Activity Logging

Policy and Charging Rules Function (PCRF)

PCRF 1.6.0 has been updated with the following enhancements:

- Custom AVP to support 3rd party vendor specific AVPs.
- Upgrade Enhancements
- Session Viewer
- Diameter Gateway scaling

Service Communication Proxy (SCP)

SCP 1.6.0 has been updated with the following enhancements:

- Support of ATS framework with test cases of SCP functionality.
- Support for networks with multiple PLMN regional NRFs.
- Compliant with Release 15 September'19 version (CHF and UDR) keeping backward compatibility with Release 15.2:
  - CHF
    * Nchf_SpendingLimitControl
    * Nchf_ConvergedCharging
  - UDR
    * Nudr_DataRepository

Security Edge Proxy Protection (SEPP)

SEPP 1.3.0 has been updated with the following enhancements:

- IPX proxy mode with modification policy support (Only Http2 with single Roaming Partner).

Unified Data Management (UDM)

There are no new features/updates implemented in CNC 2.2.0 release.

Unified Data Repository (UDR)

UDR 1.6.0 has been updated with the following enhancements:

- Support for PCF data with 3GPP Release 16 (TS29.519 v16.2.0).
- Support TLS for ingress traffic.
- Integrated with ProvGw application for SLF provisioning.
- Integrated with CNC-Console for provisioning operations.

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 Oracle Help Center (OHC). 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 2.2.0. 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 2.2.0

Part Number	Description
NA	Oracle Communications Cloud Native Core Automated Testing Suite (ATS) 1.1.0
NA	Oracle Communications Cloud Native Core Binding Support Function (BSF) 1.4.0
NA	Oracle Communications Cloud Native Core Console (CNCC) 1.1.0
NA	Oracle Communications Cloud Native Core Cloud Native Environment (CNE) 1.4.0
NA	Oracle Communications Cloud Native Core Diameter Routing Agent (CnDRA) 1.6.0
NA	Oracle Communications Cloud Native Core Inter-Working Function (IWF) 1.4.1
NA	Oracle Communications Cloud Native Core Network Exposure Function (NEF) 1.2.0
NA	Oracle Communications Cloud Native Core Network Repository Function (NRF) 1.6.1
NA	Oracle Communications Cloud Native Core Network Repository Function (NRF) 1.6.0
NA	Oracle Communications Cloud Native Core Network Slice Selection Function (NSSF) 1.3.0
NA	Oracle Communications Cloud Native Core Policy and Charging Rules Function (PCRF) 1.6.0
NA	Oracle Communications Cloud Native Core Policy Control Function (PCF) 1.6.1
NA	Oracle Communications Cloud Native Core Service Communication Proxy (SCP) 1.6.0

Table 3-1   (Cont.) Media Pack Contents for Cloud Native Core 2.2.0

Part Number	Description
NA	Oracle Communications Cloud Native Core Security Edge Protection Policy (SEPP) 1.3.0
NA	Oracle Communications Cloud Native Core Unified Data Repository (UDR) 1.6.0
NA	Oracle Communications Cloud Native Core Unified Data Management (UDM) 1.1.0

Load Line Up for Cloud Native Core

Cloud Native Core Release 2.2.0

Cloud Native Core Release 2.2.0 contains the following components:

Table 3-2   Load Line Up for Cloud Native Core

Components	Versions
Automated Testing Suite	1.1.0
Binding Support Function	1.4.0
Cloud Native Environment	1.4.0
Cloud Native Core Console	1.1.0
Cloud Native Diameter Routing Agent	1.6.0
Inter-Working Function	1.4.1
Network Exposure Function	1.2.0
Network Repository Function	1.6.1
Network Repository Function	1.6.0
Network Slice Selection Function	1.3.0
Policy and Charging Rules Function	1.6.0
Policy Control Function	1.6.1
Service Communication Proxy	1.6.0
Security Edge Proxy Protection	1.3.0
Unified Data Repository	1.6.0
Unified Data Management	1.1.0

Documentation Pack

All documents are available for download from the Oracle Help Center (OHC) site.

4

Resolved and Known Bugs

This chapter lists the resolved and known bugs for Cloud Native Core release 2.2.0.

These lists are distributed to customers with a new software release at the time of General Availability (GA) and are updated for each maintenance release.

Severity Definitions

Service requests for supported Oracle programs may be submitted by you online through Oracle's web-based customer support systems or by telephone. The service request severity level is selected by you and Oracle and should be based on the severity definitions specified below.

Severity 1

Your production use of the supported programs is stopped or so severely impacted that you cannot reasonably continue work. You experience a complete loss of service. The operation is mission critical to the business and the situation is an emergency. A Severity 1 service request has one or more of the following characteristics:

- Data corrupted.
- A critical documented function is not available.
- System hangs indefinitely, causing unacceptable or indefinite delays for resources or response.
- System crashes, and crashes repeatedly after restart attempts.

Reasonable efforts will be made to respond to Severity 1 service requests within one hour. For response efforts associated with Oracle Communications Network Software Premier Support and Oracle Communications Network Software Support & Sustaining Support, please see the Oracle Communications Network Premier & Sustaining Support and Oracle Communications Network Software Support & Sustaining Support sections above.

Except as otherwise specified, Oracle provides 24 hour support for Severity 1 service requests for supported programs (OSS will work 24x7 until the issue is resolved) when you remain actively engaged with OSS working toward resolution of your Severity 1 service request. You must provide OSS with a contact during this 24x7 period, either on site or by phone, to assist with data gathering, testing, and applying fixes. You are requested to propose this severity classification with great care, so that valid Severity 1 situations obtain the necessary resource allocation from Oracle.

Severity 2

You experience a severe loss of service. Important features are unavailable with no acceptable workaround; however, operations can continue in a restricted fashion.

Severity 3

You experience a minor loss of service. The impact is an inconvenience, which may require a workaround to restore functionality.

Severity 4

You request information, an enhancement, or documentation clarification regarding your software but there is no impact on the operation of the software. You experience no loss of service. The result does not impede the operation of a system.

Resolved Bug List

The following Resolved Bugs tables list the bugs that are resolved in Cloud Native Release 2.2.0.

Table 4-1   NRF 1.6.1 Resolved Bugs

Bug Number	Severity	Found in Release	Title
31380120	2	1.5.1	NRF's Ingress-Gateway PODs becomes unresponsive after processing HTTP/1.x message
31380143	3	1.5.1	NRF's Egress-Gateway through's Connection Error Exception after a Idle 15 minutes Timeout between NRF and SLF connection

Table 4-2   NRF 1.6.0 Resolved Bugs

Bug Number	Severity	Found in Release	Title
30995372	4	1.5.0	NRF Latency metrics should be pegged even when processing time is less than 0 milliseconds (i.e. if the value is in microseconds)

Table 4-3   SCP 1.6.0 Resolved Bugs

Bug Number	Severity	Found in Release	Title
30731829	3	1.4.0	SCPC-Pilot is taking high CPU while applying updates if number of equivalent profiles/ServiceInstances are exceeding 100
31315602	3	1.5.0	SCP to alert if 2xx is received in Audit with empty array for discovery or management

Table 4-4   UDR 1.6.0 Resolved Bugs

Bug Number	Severity	Found in Release	Title
30720600	4	1.5.0	UDR notify service keeps triggering notification for single modification of any resources(eg AM_DATA)

Table 4-5   CNDRA 1.6.0 Resolved Bugs

Bug Number	Severity	Found in Release	Title
30542078	3	1.4.0	Enabling 1k/ pod diameter connections, causes invalid fd issue on draworker pod

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 4-6   NRF 1.6.1 Customer Known Bugs

Bug Number	Severity	Found in Release	Title	Customer Impact
31331560	4	1.5.0	NRF is not validating unique serviceInstanceId	NFs should refrain sending duplicate serviceInstanceId.
31331608	4	1.5.1	Cachecontrol header is not being sent in forwarded discovery response	Intermediate Proxies cannot cache the Discovery Response.

Table 4-7   NRF 1.6.0 Customer Known Bugs

Bug Number	Severity	Found in Release	Title	Customer Impact
31331560	4	1.5.0	NRF is not validating unique serviceInstanceId	NFs should refrain sending duplicate serviceInstanceId.
31331608	4	1.5.1	Cachecontrol header is not being sent in forwarded discovery response	Intermediate Proxies cannot cache the Discovery Response.
31380120	2	1.5.1	NRF's Ingress-Gateway PODs becomes unresponsive after processing HTTP/1.x message	Ingress-Gateway POD will not be able to process any request until the POD restarts.

Table 4-7   (Cont.) NRF 1.6.0 Customer Known Bugs

Bug Number	Severity	Found in Release	Title	Customer Impact
31380143	3	1.5.1	NRF's Egress-Gateway through's Connection Error Exception after a Idle 15 minutes Timeout between NRF and SLF connection	If the NRF-SLF connection remains idle for 15 mins, upto 4 initial SLF query will fail. Subsequent SLF requests will pass until there is no 15 mins idle time.

Table 4-8   SCP 1.6.0 Customer Known Bugs

Bug Number	Severity	Found in Release	Title	Customer Impact
30731782	3	1.2.0	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 and hence minimal impact for customer/user. **Workaround**: None. This is limited by underlying platform.
30731844	3	1.3.0	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. **Workaround**: None.

Table 4-9   UDR 1.6.0 Customer Known Bugs

Bug Number	Severity	Found in Release	Title	Customer Impact
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.

Table 4-9   (Cont.) UDR 1.6.0 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.
31330261	4	1.6.0	UDR allows creating SLF data with empty nfGroupId	No impact.
31330361	3	1.6.0	Error response format from ProvGw is not as expected.	No impact. Needs error code enhancement
31330332	3	1.6.0	ProvGw does not send to second UDR within same segment.	**Workaround**: Configure all UDR FQDNs in the segments list in the values.yaml file.

Table 4-10   PCRF 1.6.0 Customer Known Bugs

Bug Number	Severity	Found in Release	Title	Customer Impact
31319315	2	CnPCRF 1.6.0	cnPCRF 1.6: Connection from Diam-GW to external SPR servers requires a core restart	**Workaround**: A restart of the core process.
31319428	3	CnPCRF 1.6.0	cnPCRF 1.6: No Options available to disable combine lookup and subscription for UDR data source	**Workaround**: None.
31319500	2	CnPCRF 1.6.0	cnPCRF 1.6: Unable to see policies in GUI after a Bulk import options	**Workaround**: Manual Creation.
31320395	3	CnPCRF 1.6.0	cnPCRF 1.6.0: Some types are missed on the page of Diameter peer nodes cfg making it unusable	Using the Kubernetes config map for the peer configuration.
31326154	4	CnPCRF 1.6.0	Getting 500 error while searching session by IPV6 if excessive space given after actual search value	**Workaround**: Remove excessive space from search text and try searching again.
31370072	3	CnPCRF 1.6.0	cnPCRF 1.6.0 : Diameter Gateway is not initiating connection towards OCS when one creates Peer Node from CM GUI	**Workaround**: Don't configure Peer from CM GUI and configure it in ConfigMap

Table 4-11   PCF 1.6.0 Customer Known Bugs

Bug Number	Severity	Found in Release	Title	Customer Impact
31366879	3	1.6	PCF: SM-service is not able to handle the request when PRE sends to to install Session Rule mapped to a Session Rule Profile	If PCF installed the session rule with ID as "sess1" and we want to override some of the parameters by keeping the same session rule ID by applying Session rule profile parameters. Currently SM-service is throwing exception while getting the request from PRE to override the session rule profile. **Workaround**: We can install new session rule with a different ID.
31366969	3	1.6	PRE evaluation: PRE evaluation throws error in case blockly access an object that is not present	Policy evaluation will fail in case blockly access an object that is not present. **Workaround**: To use Object expression block to validate the object against NULL, before using the object.
31367038	3	1.6	Remove clusterRole and ClusterRoleBinding from Policy solution	**Workaround**: None.
31367115	3	1.6	Bulk Import export does not work with Overwrite Option	User will not be able to do Bulk Import with Overwrite option. **Workaround**: Bulk Import can be used with Delete Option.

Table 4-12   CNCC 1.1.0 Customer Known Bugs

Bug Number	Severity	Found in Release	Title	Customer Impact
31355467	3	1.1.0	CNCC UDR screen - Minor issue in displaying error message having long text	**Workaround**: None.
31355421	3	1.1.0	CNCC UDR Screen - Open Items	**Workaround**: Direct API call can be made.

Table 4-12   (Cont.) CNCC 1.1.0 Customer Known Bugs

Bug Number	Severity	Found in Release	Title	Customer Impact
31367038	3	1.1.0	Remove clusterRole and ClusterRoleBinding from Policy solution	**Workaround**: None.
31355443	3	1.1.0	CNCC UDR Screen - Not displaying Authentication Error Messages	Error window will get popped up but no message will be displayed in case of unauthorized access. **Workaround**: None.
31355530	3	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. **Workaround**: Delete user and recreate user with required role.

Table 4-13   ATS 1.1.0 Customer Known Bugs

Bug Number	Severity	Found in Release	Title	Customer Impact
31377981	3	OCNRF 1.6.0	NRF ATS 1.1.0 can't be deployed using Helm3	**Workaround**: Either use helm2 to deploy or update the app version in deployment file of ATS helm charts.