

Oracle® Communications

Cloud Native Core Release Notice



Release 2.0.0

F22872-02

February 2020

The Oracle logo, consisting of a solid red square with the word "ORACLE" in white, uppercase, sans-serif font centered within it.

ORACLE®

Oracle Communications Cloud Native Core Release Notice, Release 2.0.0

F22872-02

Copyright © 2019, 2020, Oracle and/or its affiliates. All rights reserved.

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

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

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

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

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

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

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

Contents

1 Introduction

Documentation Admonishments	1-1
Locate Product Documentation on the Oracle Help Center Site	1-1
Customer Training	1-2
My Oracle Support	1-2
Emergency Response	1-2

2 Feature Descriptions

Cloud Native Core Applications, Release 2.0.0	2-1
Oracle Communications- Cloud Native Environment (OC-CNE)	2-1
Unified Data Repository (UDR)	2-1
Network Repository Function (NRF)	2-2
Inter-Working Function (IWF)	2-2
Binding Support Function (BSF)	2-3
Service Communication Proxy (SCP)	2-3
Network Exposure Function (NEF)	2-3
Security Edge Proxy Protection (SEPP)	2-4
Network Slice Selection Function (NSSF)	2-4
Cloud Native Diameter Routing Agent (CNDRA)	2-4
Policy Control Function (PCF)	2-5
Policy and Charging Rules Function (PCRF)	2-5

3 Media and Documentation

Media Pack	3-1
Load Line Up for Cloud Native Core	3-2
Documentation Pack	3-2

4 Resolved and Known Bugs

Severity Definitions	4-1
Resolved Bug List	4-2

List of Tables

1-1	Admonishments	1-1
3-1	Media Pack Contents for Cloud Native Core	3-1
3-2	Load Line Up for Cloud Native Core	3-2
3-3	Documentation Pack Contents	3-2
4-1	Cloud Native Release 1.0.0 Resolved Bugs	4-2
4-2	Cloud Native Core Customer Known Bugs	4-2

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 Oracle 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.




5G Cloud Native Core Release 2.0.0 Introduction

Oracle Communications Cloud Native network functions debut with this release. Each of the new network functions are described in [Feature Descriptions](#) under their respective Cloud Native headings. These functions allow you to access the database for storing application, subscription, authentication, service authorization, policy data, session binding, and application state information.

Documentation Admonishments

Admonishments are icons and text throughout this manual that alert the reader to assure personal safety, to minimize possible service interruptions, and to warn of the potential for equipment damage.

Table 1-1 Admonishments

Icon	Description
 DANGER	Danger: (This icon and text indicate the possibility of personal injury.)
 WARNING	Warning: (This icon and text indicate the possibility of equipment damage.)
 CAUTION	Caution: (This icon and text indicate the possibility of service interruption.)

Locate Product Documentation on the Oracle Help Center Site

Oracle Communications customer documentation is available on the web at the Oracle Help Center site, <http://docs.oracle.com>. You do not have to register to access these documents. Viewing these files requires Adobe Acrobat Reader, which can be downloaded at <http://www.adobe.com>.

1. Access the Oracle Help Center site at <http://docs.oracle.com>.
2. Click **Industries**.
3. Under the Oracle Communications subheading, click **Oracle Communications documentation** link.
The Communications Documentation page displays.
4. Click on your product and then the release number.
A list of the documentation set for the selected product and release displays.
5. To download a file to your location, right-click the **PDF** link, select **Save target as** (or similar command based on your browser), and save to a local folder.

Customer Training

Oracle University offers training for service providers and enterprises. Visit our web site to view, and register for, Oracle Communications training at <http://education.oracle.com/communication>.

To obtain contact phone numbers for countries or regions, visit the Oracle University Education web site at www.oracle.com/education/contacts.

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.

Emergency Response

In the event of a critical service situation, emergency response is offered by the Customer Access Support (CAS) main number at 1-800-223-1711 (toll-free in the US), or by calling the Oracle Support hotline for your local country from the list at <http://www.oracle.com/us/support/contact/index.html>. The emergency response provides immediate coverage, automatic escalation, and other features to ensure that the critical situation is resolved as rapidly as possible.

A critical situation is defined as a problem with the installed equipment that severely affects service, traffic, or maintenance capabilities, and requires immediate corrective action. Critical situations affect service and/or system operation resulting in one or several of these situations:

- A total system failure that results in loss of all transaction processing capability
- Significant reduction in system capacity or traffic handling capability
- Loss of the system's ability to perform automatic system reconfiguration
- Inability to restart a processor or the system
- Corruption of system databases that requires service affecting corrective actions
- Loss of access for maintenance or recovery operations
- Loss of the system ability to provide any required critical or major trouble notification

Any other problem severely affecting service, capacity/traffic, billing, and maintenance capabilities may be defined as critical by prior discussion and agreement with Oracle.

2

Feature Descriptions

This chapter provides a summary of each feature released in Cloud Native Core features releases 2.0.0.

Cloud Native Core Applications, Release 2.0.0

Oracle Communications Cloud Native Core is a market-leading core network solution utilizing Cloud Native principles and architecture to deliver Service Agility, Innovation, Efficiency and Adaptability for 4G and 5G network functions including an optional on premise Cloud Native Environment.

Oracle Communications- Cloud Native Environment (OC-CNE)

Oracle Communications- Cloud Native Environment (OC-CNE) is an on-premises cloud native environment comprised of a collection of services sponsored by the CNCF that delivers a common mechanism for the operation and maintenance of applications. This includes the following categories:

- Runtime services (container management and networking)
- Orchestration and management services
- Storage services
- Security services
- Observability services (logging, tracing, and metrics)
- DevOps services (continuous integration and continuous deployment automation): not part of this release

Here is a list of OC-CNE services:

- Support CNE on top of bare metal infrastructure
- Support CGBU 5G NF deployments, scaling, and un-deployment use cases
- Provide common services for all 5G NFs (metrics, logging and tracing)
- Installation of DB tier for configuration storage
- Basic security for OL, Kubernetes, IP layer, and DB storage
- Network segregation for OAM and Signaling traffic

CNCF is an open source software foundation dedicated to making cloud native computing universal and sustainable.

Unified Data Repository (UDR)

Oracle 5G Unified Data Repository (UDR), implemented as cloud native function, offers a unified database for storing application, subscription, authentication, service authorization,

policy data, session binding, and application state information. The 5G UDR is a key component of the 5G service-based architecture and provides an HTTP/2 RESTful interface for other network functions (NFs) and provisioning clients to access the data. Other advantages of Oracle's 5G UDR include:

- A common Oracle Communications cloud native framework.
- Compliant with 3GPP release 15 specifications.
- Tiered architecture providing separation between the connectivity, business logic and data layers.
- MySQL NDB cluster as the backend database in the data tier.
- Registers with NRF in the 5G network, so the other NFs in the network can discover UDR through Network Repository Function.

Note : UDR supports only PCF data in this initial release.

UDSF (Unstructured Data Storage Function) is the functionality that supports storage and retrieval of unstructured data by any 5G NF. 3GPP does not define UDSF specifications. This functionality is part of Oracle's 5G UDR solution.

For more information, refer to *Unified Data Repository User's Guide* under Cloud Native documents on OHC.

Network Repository Function (NRF)

The Network Repository Function (NRF) is a key component of the 5G service-based architecture. The NRF maintains an updated repository of all the 5G elements available in the operator's network along with the services provided by each of the elements in the 5G core that are expected to be instantiated, scaled, and terminated without, or have minimal, manual intervention. In addition to serving as a repository of the services, the NRF also supports discovery mechanisms that allow 5G elements to discover each other and get an updated status of the desired elements.

The NRF supports the following functions:

- Maintains the profiles of the available NF instances and their supported services in the 5G core network.
- Allows consumer NF instances to discover other provider's NF instances in the 5G core network.
- Allows NF instances to track the status of other NF instances.

For more information, refer to *Network Repository Function User's Guide* under Cloud Native documents on OHC.

Inter-Working Function (IWF)

The Oracle 5G Inter-Working Function (IWF) is deployed as an independent network function in the 5G core network or as part of the Oracle 5G core NF including the NRF, Security Edge Protection Proxy (SEPP), and Service Communication Proxy (SCP) as an independent micro service.

The key capabilities of the IWF include:

Protocol Translation:

- Allows the 5GC NF to interwork with the EPC network elements

- Supports Diameter to HTTP/2 protocol conversion capabilities

Message Mediation:

- Allows API transformation to resolve inter-NF inter-operational issues
- Allows users to create policy rules to execute mediation transformation

For more information, refer to *Inter-Working Function User's Guide* under Cloud Native documents on OHC.

Binding Support Function (BSF)

The Binding Support Function allows Policy Control Function (PCF) to register, update, and remove the binding information from it; and allows NF consumers to discover the selected Policy Control Function.

The Binding Support Function stores the binding information for a certain Protocol Data Unit (PDU) sessions and discovers the selected PCF according to the binding information. It also acts as Diameter proxy agent or Diameter redirect agent to Rx requests targeting an IP address of the User Equipment (UE) to the selected PCF.

For any application function using Rx, such as P-CSCF, the Binding Support Function determines the selected PCF address according to the information carried by the incoming Rx requests.

For more information, refer to *Binding Support Function User's Guide* under Cloud Native documents on OHC.

Service Communication Proxy (SCP)

The core network in 5G follows a Service Based Architecture where network elements advertise and provide services that can be consumed using REST APIs by other elements in the core. This allows for the adoption of web-scale technologies and software that are used by different organizations in telecom networks. Web-scale technologies rely primarily on open source software and bring in a significant amount of automation, prominently in the deployment and operational aspects. To resolve issues such as Congestion Control, Traffic Prioritization, Overload Control, Optimized Routing, several software solutions, referred to as service mesh, are being developed as part of web-scale technologies. However, these solutions are based on information elements present in messages below the telecom layer and hence not telecom aware.

The Oracle Communications Service Communication Proxy brings telecom awareness to the service mesh and helps resolve the above-mentioned issues in the 5G core network.

For more information, refer to *Service Communication Proxy User's Guide* under Cloud Native documents on OHC.

Network Exposure Function (NEF)

The Network Exposure Function (NEF) is a functional element that supports the following functionalities:

- Securely exposes network capabilities and events provided by 3GPP NFs to application function (AF).
- Provides a means for the AF to securely provide information to 3GPP network and may authenticate, authorize, and assist in throttling the AF.

- Exposes information collected from other 3GPP NFs to the AF.
- Translates the information between the AF and internal 3GPP NFs.
- Supports a Packet Flow Description (PFD) Function, which allows the AF to provision PFDs and may store and retrieve PFDs in the UDR. The NEF further provisions PFDs to the Session Management Function.

A specific NEF instance may support one or more of the functionalities described and, consequently, an individual NEF may support a subset of the APIs specified for capability exposure.

For more information, refer to *Network Exposure Function User's Guide* under Cloud Native documents on OHC.

Security Edge Proxy Protection (SEPP)

Security Edge Protection Proxy (SEPP) is a proxy network functional element used for secured communication between inter-PLMN network messages.

For more information, refer *Security Edge Protection Proxy User's Guide* under Cloud Native documents on OHC.

Network Slice Selection Function (NSSF)

The Network Slice Selection Function (NSSF) is a functional element that supports these functionalities:

- The Access and Mobility Management Function (AMF) performs initial registration and protocol data unit (PDU) session establishment.
- Using the Network Slicing Instance (NSI), NSSF determines the authorized Network Slice Selection Assistance Information (NSSAI) and AMF to serve the UE AMF, which can retrieve the NRF, NSI ID, and target AMFs as part of UE initial registration and PDU establishment procedure.
- Interaction with NRF to retrieve specific NF services to use for registration requests.

For more information, refer to *Network Slice Selection Function User's Guide* under Cloud Native documents on OHC.

Cloud Native Diameter Routing Agent (CNDRA)

(Optional) Enter reference information in this section.

The Cloud Native Diameter Routing Agent (CNDRA) is Diameter Routing solution for the Cloud Native Environment. The CNDRA supports the following features:

- Initial deployment is performed using Helm Job.
- MMI support for Diameter configuration.
- Logging support through CNE infrastructure components, such as EFK.
- Responder connection support for any message processor PODs (draWorker) in the topology.
- Peer's incoming connection requests is distributed using MetalLB (Cluster level) and subsequently by Kube-proxy (Node level) to an mpPod in the topology.

- Initiator connection distribution support with Pod having least number of initiator connections available in topology.

For more information, refer to *Cloud Native Diameter Routing Agent (CNDRA) Installation Guide*.

Policy Control Function (PCF)

The Oracle Communications Policy Management solution is enhanced to add Policy Control Function that extends the functionality of PCRF as part of 5G core network. The Policy Control Function is a functional element for policy control decision and flow based charging control functionalities. The PCF provides the following functions:

- Policy rules for application and service data flow detection, gating, QoS, and flow based charging to the SMF.
- Access and Mobility Management related policies to the AMF.

For more information, refer to *Oracle Communications Policy Control Function Cloud Native User's Guide*.

Policy and Charging Rules Function (PCRF)

The Oracle Communications Cloud Native Policy and Charging Rules Function (PCRF) solution incorporates new architecture with spring micro-service framework as backend support technology stack and Kubernetes Cloud Native Environment as running environment. The PCRF core service is the main functionality among PCRF micro services with the following enhancements when compared to legacy PCRF:

- Remove the MIA module from MPE, and let the MPE talks to with configuration server to save/load related data
- PCRF core service have integrated the MPE functionalities which are under legacy PCRF
- When PCRF Core needs to talk with any data source, these traffic shall go with the Diameter connector rather than from the PCRF core itself

For more information, refer to *Oracle Communications Policy and Charging Rules Function User's 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 Oracle Help Center (OHC). Both the software Media Pack and Documentation Pack are listed in this chapter.

Media Pack

All components available for download from the Oracle Software Delivery Cloud (<https://edelivery.oracle.com/>) are in Table 3-1.

 **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

Part Number	Description
V983767-01	Oracle Communications Binding Support Function (BSF) 1.0.0.0.0
V983600-01	Oracle Communications Inter-Working Function (IWF) 1.0.0.0.0
V983601-01	Oracle Communications Network Exposure Function (NEF) 1.0.0.0.0
V983602-01	Oracle Communications Network Repository Function (NRF) 1.0.0.0.0
V983603-01	Oracle Communications Network Slice Selection Function (NSSF) 1.0.0.0.0
V983604-01	Oracle Communications Security Edge Protection Proxy (SEPP) 1.0.0.0.0
V983537-01	Oracle Communications Service Communication Proxy (SCP) 1.0.0.0.0
V983533-01	Oracle Communications Unified Data Repository (UDR) 1.0.0.0.0
V983520-01	Oracle Communications Cloud Native Diameter Routing Agent 1.0.0.0.0
V983517-01	Oracle Communications Cloud Native Environment 1.0.1.0.0
V983519-01	Oracle Communications Policy and Charging Rules Function 1.0.0.0.0
V983768-01	Oracle Communications Policy Control Function 1.0.0.0.0

Load Line Up for Cloud Native Core

Cloud Native Core Release 2.0.0 contains the following components:

Table 3-2 Load Line Up for Cloud Native Core

Components	Versions
Binding Support Function	1.0.0.0.0
Inter-Working Function	1.0.0.0.0
Network Exposure Function	1.0.0.0.0
Network Repository Function	1.0.0.0.0
Network Slice Selection Function	1.0.0.0.0
Security Edge Proxy Protection	1.0.0.0.0
Service Communication Proxy	1.0.0.0.0
Unified Data Repository	1.0.0.0.0
Cloud Native Diameter Routing Agent	1.0.0.0.0
Cloud Native Environment	1.0.1.0.0
Policy and Charging Rules Function	1.0.0.0.0
Policy Control Function	1.0.0.0.0

Documentation Pack

All documents available for download from the Oracle Help Center (OHC) site (<http://docs.oracle.com/en/industries/communications/>) are listed in Table 3-3.

 **Note:**

This list is accurate at the time of release, but it is subject to change. See the Oracle Help Center for the latest information.

Table 3-3 Documentation Pack Contents

Release Notices and Licensing Information User Manuals Document Set
Cloud Native Core Release Notice
Cloud Native Core Licensing Information User Manual
Cloud Native Core Installation Document Set
CNE Installation Guide and ZIP file containing Grafana dashboard JSON file and Alert configuration file
Cloud Native Diameter Routing Agent (cnDRA) Installation Guide and ZIP file containing Grafana dashboard JSON file and Alert configuration file
Binding Support Function (BSF) Installation and Upgrade Guide

Table 3-3 (Cont.) Documentation Pack Contents

Inter-Working Function (IWF) Installation Guide and ZIP file containing Grafana dashboard JSON file and Alert configuration file
Network Exposure Function (NEF) Installation and Upgrade Guide
Network Repository Function (NRF) Installation and Upgrade Guide and ZIP file containing Grafana dashboard JSON file and Alert configuration file
Network Slice Selection Function (NSSF) Installation Guide and ZIP file containing Grafana dashboard JSON file and Alert configuration file
Service Communication Proxy (SCP) Installation Guide and ZIP file containing Grafana dashboard JSON file and Alert configuration file
Security Edge Proxy Protection (SEPP) Installation Guide and ZIP file containing Grafana dashboard JSON file and Alert configuration file
Unified Data Repository (UDR) Installation and Upgrade Guide, REST Cloud Native Specification Document, and ZIP file containing Grafana dashboard JSON file and Alert configuration file
Policy Control Function (PCF) Installation and Upgrade Guide
Policy and Charging Rules Function (PCRF) Installation and Upgrade Guide
Cloud Native Core Document Set
Binding Support Function (BSF) User's Guide
Inter-Working Function (IWF) User's Guide
Network Repository Function (NRF) User's Guide
Network Slice Selection Function (NSSF) User's Guide
Service Communication Proxy (SCP) User's Guide
Security Edge Proxy Protection (SEPP) User's Guide
Unified Data Repository (UDR) User's Guide
Policy Control Function (PCF) User's Guide
Policy and Charging Rules Function (PCRF) User's Guide

4

Resolved and Known Bugs

This chapter lists the resolved and known bugs for Cloud Native Core release 2.0.0.

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

The problem report sections in this document refer to bug severity levels. Definitions of these levels can be found in the publication, *TL 9000 Quality Management System Measurement Handbook*.

Problem Report: A report from a customer or on behalf of the customer concerning a product or process defect requesting an investigation of the issue and a resolution to remove the cause. The report may be issued via any medium.

Problem reports are systemic deficiencies with hardware, software, documentation, delivery, billing, invoicing, servicing, or any other process involved with the acquisition, operation, or performance of a product. An incident reported simply to request help to bring back the service or functionality to normal without the intent to investigate and provide a resolution to the cause of the incident is not a problem report.

- 1. Critical:** Conditions that severely affect the primary functionality of the product and because of the business impact to the customer requires non-stop immediate corrective action regardless of time of day, or day of the week as viewed by a customer on discussion with the organization such as:
 - Product inoperability (total or partial outage),
 - A reduction in the capacity capability, that is, traffic/data handling capability, such that expected loads cannot be handled,
 - Any loss of emergency capability (for example, emergency 911 calls), or
 - Safety hazard or risk of security breach.
- 2. Major:** Product is usable, but a condition exists that seriously degrades the product operation, maintenance, or administration, etc., and requires attention during pre-defined standard hours to resolve the situation.
The urgency is less than in critical situations because of a less immediate or impending effect on product performance, customers, and the customer's operation and revenue such as:
 - Reduction in product's capacity (but still able to handle the expected load),
 - Any loss of administrative or maintenance visibility of the product and/or diagnostic capability,
 - Repeated degradation of an essential component or function, or
 - Degradation of the product's ability to provide any required notification of malfunction.

- Minor:** Other problems of a lesser severity than "critical" or "major" such as conditions that have little or no impairment on the function of the system.

The numbered severity levels in the tables below correspond to these definitions of 1-Critical, 2-Major, or 3-Minor.

Resolved Bug List

Table 4-1 lists bugs resolved in this release.

Table 4-1 Cloud Native Release 1.0.0 Resolved Bugs

Bug Number	Severity	Found in Release	Title
29631361	2	1.0.0	NF CNE Installation Issues with HP Gen10 hardware Note: This only impacts installation on HP Gen10 hardware.

Customer Known Bug List

Table 4-2 lists the known bugs and associated Customer Impact Statements. This information is provided for information purposes only.

Table 4-2 Cloud Native Core Customer Known Bugs

Bug Number	Severity	Found in Release	Title	Customer Impact
29623007	4	1.0.0	NRF creating duplicate subscription	Duplicate notification is received by the client in case it has sent a duplicate subscription request. Workaround : None
29623203	3	1.0.0	GET ALL (NF Instances) response is not having _links object	GET All response can't be used as it is. Workaround : Client needs to fetch the URL directly from the response body (vs fetching it from _link attribute) or alternately use Discovery service to fetching NF profiles.
29623333	4	1.0.0	GET ALL (NF Instances) request is not handling optional parameters	nf-type and limit optional parameter can't be used for GET ALL request. Workaround : None.
29631361	3	1.0.0	NF CNE installation issues with HP Gen10 hardware	Results in incorrect cluster configuration. However, the issues can be resolved and/or corrected manually.
29622977	3	1.0.0	Virtual services are not getting updated or deleted when non-equivalent NF services registered with overlapping IP endpoints	Rules will not flow down to worker for routing if 2 NF/NF-Service registered or updated with same set of IP endpoints. Workaround : Make sure no NFs or their services are configured with same set of IP endpoints.

Table 4-2 (Cont.) Cloud Native Core Customer Known Bugs

Bug Number	Severity	Found in Release	Title	Customer Impact
29622956	3	1.0.0	NullPointerException occurs in notification module when de-register comes immediately after register	In case NF deregister comes immediately after NF register this problem will come and De register will not happen. Workaround : Resend de-register notification from NRF or make sure de-register does not immediately follow register.
29622946	4	1.0.0	Failure to process consecutive NF_REGISTERED event with same NF but different NF profile	None. Consecutive profile for same NF Instance ID with different NF type is not processed. Workaround : None. Ideally NF Instance ID from different NF types should be different.