Oracle® Communications

Cloud Native Core Release Notice

Release 2.1.1

F29511-06

June 2020

Oracle Communications Cloud Native Core Release Notice, Release 2.1.1

F29511-06

Contents

List of Tables

1

What's New In This Guide

New and Updated Features

Following section is updated for SCP Releases 1.5.3:

- Resolved Bug List
- Customer Known Bug List
- Media and Documentation

New and Updated Features

Following section is updated for IWF Releases 1.4.1:

- Resolved Bug List.

New and Updated Features

Following sections are updated for PCF Releases 1.5.1 and 1.5.2:

- Resolved Bug List.
- Policy Control Function (PCF).

New and Updated Features

Following section is updated for SCP Release 1.5.2:

- Resolved Bug List.

New and Updated Features

Following sections are updated for NRF Release 1.5.1 and SCP Release 1.5.1:

- Network Repository Function (NRF).
- Resolved Bug List.

2
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.

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 2-1 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*.)
TOPPLE	Topple: (This icon and text indicate the possibility of *personal injury* and *equipment damage*.)

Locate Product Documentation on the Oracle Help Center Site

Oracle Communications customer documentation is available on the web at the Oracle Help Center (OHC) 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 the **Industries** link. The **Industries Documentation** page displays.

3. Click the `Oracle Communications` link.

   The **Communications** Documentation page appears. Most products covered by these documentation sets will appear under the headings **Signaling and Policy**.

4. Click on your Product and then the Release Number.

   A list of the entire documentation set for the selected product and release appears.

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.

3

Feature Descriptions

This chapter provides a summary of each feature released in Cloud Native features release 2.1.1.

Cloud Native Environment (OC-CNE)

OC-CNE 1.4 has been updated with the following enhancements:

- **Continuous Deployment**

  OC-CNE 1.4 includes a Continuous Deployment (CD) pipeline to automate OC-CNE lifecycle operations.

- **Automated Upgrade**

  OC-CNE 1.4 offers a fully automated upgrade from OC-CNE 1.3. Host/guest OS, Kubernetes, and common services are all upgraded via a single CD pipeline command.

- **Automated Replication Configuration for DB Tier**
  Prior to OC-CNE 1.4, configuring cross-site DB replication was a manual process. OC-CNE 1.4 automates the initial configuration of cross-site replication.

Cloud Native Diameter Routing Agent (CnDRA)

CnDRA 1.5.0 has been updated with the following enhancements:

- Multiple deployment support for dra service
- Alert handling for pod failure

Cloud Native Core Console

Cloud Native Core Console 1.0.0 supports the following functionalities:

- Supports configuration of NRF managed objects:
  - Screening rules
  - System options
- Supports configuration of the following SCP managed objects:
  - System Options
  - Service Groups
  - SCP Profile
  - Routing Options
  - Message Priority
  - Mediation Configuration

  - Canary Release
- Integrated with PCF GUI

Binding Support Function (BSF)

The Binding Support Function 1.4.0 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.

Inter-Working Function (IWF)

IWF 1.4.0 has been updated with the following enhancements:

- To support PCF discovery to find the PCF from BSF for AAA from P-DRA

Network Exposure Function (NEF)

NEF 1.2.0 has been updated with the following enhancements:

- NEF support for Traffic Influence API and Background Data Transfer API.

Network Repository Function (NRF)

OCNRF 1.5.1 has been updated with the following enhancement:

- Support for NRF Service Operation Forwarding

OCNRF 1.5.0 has been updated with the following enhancements:

- Compliance to TS 29.510 15.5.0 (September 2019)
- Priority-handling in discovery response
- Full Address Resolution (SLF)
- Egress Gateway integration
- Integration with CNC OAM
- OCNRF ATS

Network Slice Selection Function (NSSF)

NSSF version 1.2.1 has been updated with the following enhancements:

- NS-Selection: Support for processing Subscribe and Notify (Allowing AMF to subscribe for notifications based on updates on Session data)
- NSSF supports subscription for updates on TargetAMFSet (based on TargetAMFSetId and TargetAMFRegionId) with NRF

Policy Control Function (PCF)

PCF 1.5.2 has been updated with the following enhancement:

- Compatibility of Helm chart with Kubernetes 1.16.2

The Helm chart in PCF 1.5.2 has been updated to make compatible with Kubernetes 1.16.2.

PCF 1.5.0 has been updated with the following enhancements:

- Helm Charts per Micro-service
- Enable Diameter configurations via GUI
- Horizontal Pod Autoscaler (HPA) support in PCF
- PCF HTTPS/TLS Support
- PCF Integration with CNC Core
- Session viewer support in PCF over CM API/GUI
- REST API support for PCF Configuration
- OAuth2 Support
- PCF Automated Test Suite support
- PCF Performance and stress testing/benchmarking
- PCF Stale Session Handling
- 3gpp-Sbi-Target-apiRoot header Support

Policy and Charging Rules Function (PCRF)

PCRF 1.5.0 has been updated with the following enhancements:

- CN-PCRF Policy Actions and Conditions
- Unified Policy Data Source across PCF and CN-PCRF
- Alarms and KPIs Support in CN-PCRF
- Policy Lifecycle Enhancements for cnPCRF

Service Communication Proxy (SCP)

SCP 1.5.0 has been updated with the following enhancements:

- Support to configure NF Profiles statically.
- SCP 1.5 is compliant with Release 15.2 and 15.5 versions.
  Release 15.5 support is for below services SCP only:
  - NRF Services:

        - Nnrf_NFManagement
        - Nnrf_NFDiscovery
    - UDM Services:
        - Nudm_UECM
        - Nudm_SDM
    - PCF Services:
        - Npcf_SMPolicyControl
        - Npcf_AMPolicyContro
    - AUSF Services:
        - nausf-auth
- Support for R16 3gpp-Sbi-Target-Apiroot header

Security Edge Proxy Protection (SEPP)

SEPP 1.2.0 has been updated with the following enhancements:

- SEPP compatible with OCCNE1.2/1.3

Unified Data Management (UDM)

UDM version 1.1.0 has been updated with the following enhancements:

- SIDF (Subscriber Identify De-concealing Function)
- Subscriptions and Notifications of data change towards AMF/SMF

Unified Data Repository (UDR)

UDR 1.5 has been updated with the following enhancements:

- Support for encryption of data for UDM data using MySQL NDB Cluster encryption technology
- Support for 5G SLF
- Uses 5G Ingress API gateway

Automated Testing Suite (ATS)

Automated Testing Suite (ATS) allows you to execute software test cases using an automated testing tool and then, compares the actual results with the expected or predicted results. In this process, there is no intervention from the user.

ATS for 5G Network Functions

For 5G Network Functions (NFs), ATS is built using **Oracle Linux 7-slim** as the base image. **Jenkins** is a part of the ATS image and it provides a GUI interface to the users to test either a single NF or multiple NFs independently in the same environment. Along with the NF docker images, user are provided with the ATS image, simulator images, and test cases for the specific NF. All these are handed over to the customer as a fully automated suite so that they can directly perform Lab deployment and testing. You can combine it with any other **Continuous Integration (CI) pipeline** with minimal changes, since 5G ATS uses Jenkins as GUI.

4
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 2.1.1. 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 4-1 Media Pack Contents for Cloud Native Core 2.1.1

Part Number	Description
NA	Oracle Communications Cloud Native Core Binding Support Function (BSF) 1.4.0
NA	Oracle Communications Cloud Native Core Console 1.0.0
NA	Oracle Communications Cloud Native Core Cloud Native Environment (CNE) 1.4.0
NA	Oracle Communications Cloud Native Core Diameter Routing Agent (CnDRA) 1.5.0
NA	Oracle Communications Cloud Native Core Inter-Working Function (IWF) 1.4.1
NA	Oracle Communications Cloud Native Core Inter-Working Function (IWF) 1.4.0
NA	Oracle Communications Cloud Native Core Network Exposure Function (NEF) 1.2.0
NA	Oracle Communications Cloud Native Core Network Repository Function (NRF) 1.5.1
NA	Oracle Communications Cloud Native Core Network Repository Function (NRF) 1.5.0
NA	Oracle Communications Cloud Native Core Network Slice Selection Function (NSSF) 1.2.1
NA	Oracle Communications Cloud Native Core Policy and Charging Rules Function (PCRF) 1.5.0
NA	Oracle Communications Cloud Native Core Policy Control Function (PCF) 1.5.2
NA	Oracle Communications Cloud Native Core Policy Control Function (PCF) 1.5.1

Table 4-1 (Cont.) Media Pack Contents for Cloud Native Core 2.1.1

Part Number	Description
NA	Oracle Communications Cloud Native Core Policy Control Function (PCF) 1.5.0
NA	Oracle Communications Cloud Native Core Service Communication Proxy (SCP) 1.5.3
NA	Oracle Communications Cloud Native Core Service Communication Proxy (SCP) 1.5.2
NA	Oracle Communications Cloud Native Core Service Communication Proxy (SCP) 1.5.1
NA	Oracle Communications Cloud Native Core Service Communication Proxy (SCP) 1.5.0
NA	Oracle Communications Cloud Native Core Security Edge Protection Policy (SEPP) 1.2.0
NA	Oracle Communications Cloud Native Core Unified Data Repository (UDR) 1.5.0
NA	Oracle Communications Cloud Native Core Unified Data Management (UDM) 1.1.0

Load Line Up for Cloud Native Core

Cloud Native Core Release 2.1.1

Cloud Native Core Release 2.1.1 contains the following components:

Table 4-2 Load Line Up for Cloud Native Core

Components	Versions
Binding Support Function	1.4.0
Cloud Native Core Console	1.0.0
Cloud Native Environment	1.4.0
Cloud Native Diameter Routing Agent	1.5.0
Inter-Working Function	1.4.1
Inter-Working Function	1.4.0
Network Exposure Function	1.2.0
Network Repository Function	1.5.1
Network Repository Function	1.5.0
Network Slice Selection Function	1.2.1
Policy and Charging Rules Function	1.5.0
Policy Control Function	1.5.2
Policy Control Function	1.5.1
Policy Control Function	1.5.0
Security Edge Proxy Protection	1.2.0
Service Communication Proxy	1.5.3
Service Communication Proxy	1.5.2
Service Communication Proxy	1.5.1

Table 4-2 (Cont.) Load Line Up for Cloud Native Core

Components	Versions
Service Communication Proxy	1.5.0
Unified Data Repository	1.5.0
Unified Data Management	1.1.0

Documentation Pack

All documents available for download from the Oracle Help Center (OHC) site (http://docs.oracle.com/en/industries/communications/) are listed in the Documentation Pack Contents table.

> **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 4-3 Documentation Pack Contents

Release Notices and Licensing Information User Manuals Document Set
Cloud Native Core Release Notice
Cloud Native Core Licensing Information User Manual
Automated Testing Suite (ATS)
Automated Testing Suite (ATS) Installation Guide
Binding Support Function
Binding Support Function (BSF) Installation Guide
Binding Support Function (BSF) User's Guide
Cloud Native Core Console
Cloud Native Core Console (CNCC) Installation Guide
Cloud Native Core Console (CNCC) User's Guide
Cloud Native Environment
Cloud Native Environment (CNE) Installation Guide
Cloud Native Environment (CNE) Upgrade Guide
Cloud Native Diameter Routing Agent
Cloud Native Diameter Routing Agent (cnDRA) Installation Guide
Cloud Native Diameter Routing Agent (cnDRA) User's Guide
Inter-Working Function
Inter-Working Function (IWF) Installation Guide
Inter-Working Function (IWF) User's Guide
Network Exposure Function
Network Exposure Function (NEF) Installation and Upgrade Guide
Network Repository Function
Network Repository Function (NRF) Installation and Upgrade Guide
Network Repository Function (NRF) User's Guide

Table 4-3   (Cont.) Documentation Pack Contents

Network Slice Selection Function
Network Slice Selection Function (NSSF) Installation Guide
Network Slice Selection Function (NSSF) User's Guide
Policy and Charging Rules Function
Policy and Charging Rules Function (PCRF) Installation Guide
Policy and Charging Rules Function (PCRF) User's Guide
Policy Control Function
Policy Control Function (PCF) Installation Guide
Policy Control Function (PCF) User's Guide
Policy Control Function (PCF) Cloud Native REST Specification Document
Service Communication Proxy
Service Communication Proxy (SCP) Installation Guide
Service Communication Proxy (SCP) User's Guide
Security Edge Proxy Protection
Security Edge Proxy Protection (SEPP) Installation Guide
Security Edge Proxy Protection (SEPP) User's Guide
Unified Data Repository
Unified Data Repository (UDR) Installation and Upgrade Guide
Unified Data Repository (UDR) User's Guide
Unified Data Repository (UDR) REST Cloud Native Specification Document
Unified Data Management
Unified Data Management (UDM) Installation and Upgrade Guide
Unified Data Management (UDM) User's Guide

5

Resolved and Known Bugs

This chapter lists the resolved and known bugs for Cloud Native Core release 2.1.1.

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

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.

3. **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

Cloud Native Release 2.1.1 Resolved Bugs table lists bugs resolved in this release.

Table 5-1 SCP 1.5.3 Resolved Bugs

Bug Number	Severity	Title	Found in Release	Fixed in Release
30731829	3	SCPC-Pilot is taking high CPU while applying updates if number of equivalent profiles/ServiceInstances are exceeding 100	1.4.0	1.5.3
31509529	3	Per connection TPS enhancement for SCP using IGW	1.5.0	1.5.3
31509566	3	SCP not consistently routing UECM requests based mediation rule	1.5.0	1.5.3
31509578	3	SCP does not remove a UDM profile from VS and SE after DE-Register event	1.5.0	1.5.3
31509590	2	SCP is indicating Loop Detected on NRF Notification	1.5.0	1.5.3

Table 5-2 IWF 1.4.1 Resolved Bugs

Bug Number	Severity	Title	Found in Release	Fixed in Release
31022468	3	For SCP's ResponseIngress/Egress request, NF-Mediation responding with inappropriate datatype for the attribute Status code .	1.4.0	1.4.1

Table 5-3 PCF 1.5.1 Resolved Bugs

Bug Number	Severity	Title	Found in Release	Fixed in Release
31026960	3	User-service is opening HTTP2 connection directly to UDR for sub-to-notify delete operation	1.5.0	1.5.1
31028222	3	PCF: All previously queried SM associations are returned for subsequent invalid queries	1.5.0	1.5.1

Table 5-4 SCP 1.5.2 Resolved Bugs

Bug Number	Severity	Title	Found in Release	Fixed in Release
31136820	3	TCP Reset received on connections from SCP if kept idle for >15 minutes	1.5.0	1.5.2

Table 5-5 SCP 1.5.1 Resolved Bugs

Bug Number	Severity	Title	Found in Release	Fixed in Release
31121719	2	SCP - Audit to not delete virtual services when receiving 4xx or 3xx or 5xx for a NF in audit response	1.5.0	1.5.1
31122457	2	Not all NFs are unsubscribed when changed to Local	1.5.0	1.5.1
31122469	3	SCP doesn't reroute to secondary NRF by default on 404 response	1.5.0	1.5.1
31122474	3	SCP Audit doesn't read topology source from database on audit retry after failure	1.5.0	1.5.1
31122104	2	Ignore DB error is not working for UDM Dereg callback notification	1.5.0	1.5.1
31122087	2	scp worker | Initial cluster not considered for routing when in "AlternateRouting" congestion state	1.5.0	1.5.1
31123331	3	Deployment time configuration for topology source at NF type level	1.5.0	1.5.1

Table 5-6 CNE 1.4.0 Resolved Bugs

Bug Number	Severity	Found in Release	Title
OCCNE-1543	2	1.2.0	Need add more severity values in snmp notifier.
OCCNE-1849	2	1.3.2	Post-install procedure missing instructions on required reset of DB password.
OCCNE-1646	2	1.3.2	Fix security group duplication in vCNE.
OCCNE-1706	2	1.3.2	Documentation for 1.2 Installation preflight has wrong size for Management Subnet.
OCCNE-1469	2	1.3.2	Fix fortify issue for DB tier monitor service.
OCCNE-1318	2	1.3.2	Add external IPs to SQL nodes (vCNE).

Table 5-7 NRF 1.5.0 Resolved Bugs

Bug Number	Severity	Found in Release	Title
30736715	4	1.4.0	Customer can only use default MySQL Port (3306).
30737221	4	1.4.0	No consumer NFs can ever know the when a UNDISCOVERABLE Profile becomes unavailable.

Table 5-8 IWF 1.3.0 Resolved Bugs

Bug Number	Severity	Found in Release	Title
30380965	3	1.0.0	IWF Performance Benchmark Bottleneck Analysis and improvements.

Table 5-9 PCRF 1.5.0 Resolved Bugs

Bug Number	Severity	Found in Release	Title
CNPCRF-841	3	1.4.0	cnPCRF:1.3:Dynamic pcrf-core configuration required in UDR for success response for SNR/PUR/UDR.
CNPCRF-781	3	1.4.0	pcrf-core drops requests when 'Subscription-Id-Type' is received as 'END_USER_NAI' in CCR PCRF is not taking decision based on policy counter and status received from OCS`
CNPCRF-741	3	1.4.0	Metrics were not captured by Prometheus from pcrf-core due to invalid annotations configurations in 'pcrf-core-service'
CNPCRF-732	3	1.4.0	Getting "Error: container has runAsNonRoot and image will run as root" for PRE pod
CNPCRF-653	3	1.4.0	Connection is not established when one create/update LDAP datasource from CM GUI
CNPCRF-573	3	1.4.0	LDAP Gateway is not able to connect to Config Server

Table 5-10 PCF 1.5.0 Resolved Bugs

Bug Number	Severity	Found in Release	Title
OCNGF-606	3	1.4.0	ocpm-pre service could not load the policies of wesp

Table 5-10 (Cont.) PCF 1.5.0 Resolved Bugs

Bug Number	Severity	Found in Release	Title
OCNGF-621	3	1.4.0	CM service crashed down unexpectedly
OCNGF-692	3	1.4.0	If name of Sh data source is kept 'sh' and all other mandatory fields configured , then when trying to save it throws error " Error Code 1009"
OCNGF-794	3	1.4.0	Update Policy creation to handle issues find during testing
OCNGF-795	3	1.4.0	CHF Policy changes
PCF-1234	3	1.4.0	Unsubscribe of subscriber not happening towards UDR for AM Policy delete
PCF-1295	3	1.4.0	PCF1.3 version Rx interface will return dulplicate AVPs in AAA reponse messes

Table 5-11 UDM 1.1.0 Resolved Bugs

Bug Number	Severity	Found in Release	Title
30542078	3	1.1.0	Encrypted authentication key support is not handled in UDM.

Table 5-12 UDR 1.5.0 Resolved Bugs

Bug Number	Severity	Found in Release	Title
OCUDR-562	3	1.4.0	"changes" field value is missing in the notification payload.
OCUDR-563	3	1.4.0	UDR rejects sdmSubscription creation after deleting it when SubscriptionDataSubscription already exist.

Customer Known Bug List

Cloud Native Release 2.1.1, Customer Known Bugs table lists the known bugs and associated Customer Impact Statements. This information is provided for information purposes only.

Table 5-13   CNE 1.4.0 Customer Known Bugs

Bug Number	Severity	Found in Release	Title	Customer Impact
30756164	2	1.3.2	OCCNE 1.3 Bare Metal Installation Failure -- Replication IP not configured on Sql Nodes during Db-Tier installation	The IP addresses for replication need to be configured manually following the automated installation.
30756201	4	1.3.2	OCCNE 1.3 Bare Metal Installation Failure -- Pipeline.sh is not documented. Must be continually restart on error.	An error in the installation pipeline script is not detected efficiently and requires the script to be restarted from the beginning.
30761850	2	1.3.2	DB-Tier did not recover from post weekend Lab Shutdown	DB-Tier requires manual procedure to recover from post weekend Lab Shutdown
30832402	2	1.3.2	Cisco 93180 (TOR) does not recover vrrp or port channels if DB1 fails simultaneous to loss of both TOR switches	DB-Tier requires manual procedure to recover from post weekend Lab Shutdown
30838215	2	1.3.2	OCCNE 1.3 Bare Metal Installation - Db-1 Management interface not re-configured by ansible script post pipeline	DB-Tier requires manual procedure to recover from post weekend Lab Shutdown
30936847	3	1.3.2	OCCNE 1.3 Admusr password expires after 90 days -- ssh by key stops working	ssh by key stops until password is updated
OCCNE-1265	2	1.2.0	ToR issues reset to client connections after failover	There is significant impact on a TOR switch failover if the workaround is not in place. Coordinating NAT tables between switches can be done to mitigate the impact.
OCCNE-1289	3	1.3.2	Identify the root cause in delay for VM's to come up after yum update on the host servers.	Hard coded, 5-minute, fixed delay can result in minor delay during DB Tier installation.
OCCNE-1337	3	1.3.2	k8s_install produces non-executable kubectl binary in ../artifacts	Minimal impact. This only affects verification and diagnostic procedures. There is a simple workaround that requires manual intervention.

Table 5-13 (Cont.) CNE 1.4.0 Customer Known Bugs

Bug Number	Severity	Found in Release	Title	Customer Impact
OCCNE-1398	3	1.3.2	Can't ssh to enclosure switches after configure from procedure.	Minimal impact since there is a simple workaround. The workaround is to ssh to OA then from OA "connect interconnect 1 (1 for switch1 or 2 for switch2)" to access enclosure switches.
OCCNE-1428	3	1.0.0	node_exporter generating error logs	Minor impact of an error be logged each minute from Prometheus Node Exporter.
OCCNE-1658	2	1.2.0	Pods failover takes approximately 6 mins to start when kubernetes node is failed is restarted	When a worker node fails completely or is restarted, it takes up to 7 minutes for K8s to recognize the failure and migrate the workload.
OCCNE-991	2	1.2.0	Correct osinstall yum update state	Possible significant impact if a new yum update picks up an incompatible RPM. Possible to restrict Yum channel subscription to specific channels on Bastion host and central repo.

Table 5-14 CnDRA 1.5.0 Customer Known Bugs

Bug Number	Severity	Found in Release	Title	Customer Impact
30720600	3	1.4.0	enabling 1k/ pod diameter connections, causes invalid fd issue on draworker pod	1k connections could not be configured on draworker pod.

Table 5-15 NRF 1.5.0 Customer Known Bugs

Bug Number	Severity	Found in Release	Title	Customer Impact
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)	Latency values less than 0 milliseconds will not be considered.
30995300	4	1.5.0	AdditionalAttributes are getting stored inside nfInfo objects other than the nftype's nfInfo, even when the acceptAdditionalAttributes flag is false	Additional IEs received in nfType IEs will be accepted in registration message.

Table 5-16 PCF 1.5.0 Customer Known Bugs

Bug Number	Severity	Found in Release	Title	Customer Impact
31027714	3	1.4	PCF: Unable to view CM GUI on Internet Explorer	Customer will not be able to use Internet explorer to open the CM service GUI. Customer can use other web browsers like firefox and chrome to open the CM service GUI.
31027743	3	1.4	PCF: CM GUI allows user to delete a rule/Policy that is used elsewhere	Policy evaluation will not succeed if referencing data gets deleted.
31028388	3	1.4	PCF: Rejects AAR message if RxRequestType AVP is not present	AAR message is rejected if RxRequestType AVP is not present

Table 5-17 PCRF 1.5.0 Customer Known Bugs

Bug Number	Severity	Found in Release	Title	Customer Impact
31047051	3	12.5.2.0.0	cnPCRF:1.5:Getting 'Policy execution failed: FlowChange' error if OACT_FARGO_0 is included as action in policy	**Workaround**: None.

Table 5-17   (Cont.) PCRF 1.5.0 Customer Known Bugs

Bug Number	Severity	Found in Release	Title	Customer Impact
31047021	3	12.5.2.0.0	cnPCRF:1.5:DWA result code DIAMETER_UNABLE_TO_COMPLY when pcrf-core restarted before diam-gateway	**Workaround**: None.
31046962	2	12.5.2.0.0	cnPCRF:1.5:CMGUI: Password is getting updated automatically while updating LDAP Datasource	**Workaround**: None.
31046664	2	12.5.2.0.0	cnPCRF:1.5:CCA not received when action pcc_rule with SCOPE_FLOW is used in Policy	**Workaround**: None.
31046603	3	12.5.2.0.0	cnPCRF:1.5: Sy and LDAP call-flow is not working together	**Workaround**: None.

Table 5-18   SCP 1.5.0 Customer Known Bugs

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

Table 5-19 UDR 1.5.0 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.
30774755	3	1.4.0	Headers for few resources are not implemented as per spec 29505-v15.4.0	No impact.
OCUDR-633	4	1.5.0	UDR notify service keeps triggering notification for single modification of any resources(eg AM_DATA)	Issue is seen only when client 204 result code with some content length