

Oracle® Communications

Cloud Native Core Release Notice



Release 2.1.0

F25408-02

January 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 2.1.0

F25408-02

Copyright © 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	1-2
Customer Training	1-2
My Oracle Support	1-2
Emergency Response	1-3

2 Feature Descriptions

Cloud Native Environment (OC-CNE) Version 1.3.2	2-1
Diameter Routing Agent (DRA) Version 1.4.0	2-1
Inter-Working Function (IWF) Version 1.3.0	2-1
Network Exposure Function (NEF) Version 1.2.0	2-1
Network Repository Function (NRF) Version 1.4.0	2-2
Network Slice Selection Function (NSSF) Version 1.2.0	2-2
Policy and Charging Rules Function (PCRF) Version 1.4.0	2-2
Policy Control Function (PCF) Version 1.4.0	2-2
Service Communication Proxy (SCP) Version 1.4.0	2-2
Security Edge Proxy Protection (SEPP) Version 1.2.0	2-3
Unified Data Manager (UDM)/Authentication Server Function (AUSF) Version 1.0.0	2-3
Unified Data Repository (UDR)/ Unstructured Data Storage Function (UDSF) Version 1.4.0	2-4

3 Oracle Communications Cloud Native Environment Alerts

4 Media and Documentation

Media Pack	4-1
Load Line Up for Cloud Native Core	4-2
Documentation Pack	4-2

5 Resolved and Known Bugs

Severity Definitions	5-1
Resolved Bug List	5-2
Customer Known Bug List	5-3

List of Tables

1-1	Admonishments	1-1
4-1	Media Pack Contents for Cloud Native Core 2.1.0	4-1
4-2	Load Line Up for Cloud Native Core	4-2
4-3	Documentation Pack Contents	4-2
5-1	CNE 1.3.2 Resolved Bugs	5-2
5-2	IWF 1.3.0 Resolved Bugs	5-2
5-3	NRF 1.4.0 Resolved Bugs	5-2
5-4	PCRF 1.4.0 Resolved Bugs	5-3
5-5	SCP 1.4.0 Resolved Bugs	5-3
5-6	UDR/UDSF 1.4.0 Resolved Bugs	5-3
5-7	CNE 1.3.2 Customer Known Bugs	5-3
5-8	DRA 1.4.0 Customer Known Bugs	5-5
5-9	NRF 1.4.0 Customer Known Bugs	5-5
5-10	PCF 1.4.0 Customer Known Bugs	5-5
5-11	PCRF 1.4.0 Customer Known Bugs	5-6
5-12	SCP 1.4.0 Customer Known Bugs	5-6
5-13	UDM/AUSF 1.0.0 Customer Known Bugs	5-7
5-14	UDR/UDSF 1.4.0 Customer Known Bugs	5-7

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 2.1.0 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 <i>personal injury</i> .)
 WARNING	Warning: (This icon and text indicate the possibility of <i>equipment damage</i> .)
 CAUTION	Caution: (This icon and text indicate the possibility of <i>service interruption</i> .)
 TOPPLE	Topple: (This icon and text indicate the possibility of <i>personal injury and equipment damage</i> .)

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.

2

Feature Descriptions

This chapter provides a summary of each feature released in Cloud Native Core features releases 2.1.0.

Cloud Native Environment (OC-CNE) Version 1.3.2

CNE has been updated with the following enhancements:

- Virtualized CNE. OC-CNE can be deployed on an OpenStack virtual infrastructure as well. The automated installation procedures will use OpenStack to create the virtual resources needed to host OC-CNE, and then deploy OC-CNE on those instances.
- DB Tier metrics stored in Prometheus. DB Tier metrics are collected from the DB Tier and stored in Prometheus, along with all of the other CNE metrics.
- Bare metal installation automation. The advanced installation automation used in a virtualized CNE deployment is now available for bare metal deployments as well. Once the bare metal servers are installed and initialized, much of the deployment is automated.

Diameter Routing Agent (DRA) Version 1.4.0

DRA has been updated with the following enhancements:

- Supports 100K MPS with 12 pods deployment
 - draworker default vCPU requirement has been updated from 6 vCPU to 8 vCPU
- CNDRA Upgrade Support from v1.3.3
- Logging enhancement
- Validated with CNE 1.3.2

Inter-Working Function (IWF) Version 1.3.0

IWF has been updated with the following enhancements:

- To enable test mode support in NF Mediation
- To enable response modification for responses coming from Service Communication Proxy (SCP) and Integration with SCP for response

Network Exposure Function (NEF) Version 1.2.0

NEF has been updated with the following enhancements:

- NEF support for Traffic Influence Api and Background Data Transfer Api

Network Repository Function (NRF) Version 1.4.0

NRF has been updated with the following enhancements:

- Support for AccessToken Service Operation, OAuth2.0 Support
- Support for HTTPS (TLSV1.2, Mutual)
- Support for tracing only a configurable %age of message
- Support to configure Static NodePort and Static Loadbalancer IP (if MetalLB is in use)

Network Slice Selection Function (NSSF) Version 1.2.0

NSSF 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 and Charging Rules Function (PCRF) Version 1.4.0

PCRF has been updated with the following enhancements:

- PCRF support for Presence Reporting Area
- PCRF support for IMS
- PCRF support for Multimedia Priority
- PCRF supports Time-of- Day conditions that are related to the time at which the policy rules are being executed
- To provide policy action to fetch Sy counters "fetch Policy Counter(s) default from OCS"
- To provide LDAP interface support for 3rd party UDR integration

Policy Control Function (PCF) Version 1.4.0

PCF has been updated with the following enhancements:

- PCF support for UE Route Selection Policies (URSP)
- Validated automated Test Framework for PCF
- Verified VPAT Compliance on PCF

Service Communication Proxy (SCP) Version 1.4.0

SCP has been updated with the following enhancements:

- SCP support for Policy Control Function (PCF) Npcf-am-policy-control and Npcf_UEPolicyControl in reverse proxy mode.
- SCP support for Nsmf_EventExposure service in reverse proxy and transparent proxy mode.
- SCP support for Namf_Communication service in reverse proxy and transparent proxy mode.
- To enable/update discovery response to have configured SCP IP address from all consumers of AMF services (Namf_EventExposure, Namf_Communication, AMFStatusChangeSubscribe, AMFStatusChangeUnSubscribe, AMFStatusChangeNotify)
- Performance enhancement :
 - Signaling : 3.4KMPS per worker pod
 - Capacity: verified VS creation and rules getting configured at worker for -
 - * 180 equivalent AUSF services(10service/profile) with LB for initial messages and FR with no reroute for subsequent message
 - * 18 UDM-uecm equivalent services each with 9 IPEndpoints. LB initial and subsequent messages for FR with reroute enabled
 - * 18 UDM-SDM equivalent services each with 18 IPEndpoints.LB initial and subsequent messages for FR with reroute enabled
 - * 18 UDM-EE equivalent services each with 2 IPEndpoints.LB initial and subsequent messages for FR with reroute enabled

Security Edge Proxy Protection (SEPP) Version 1.2.0

SEPP has been updated with the following enhancements:

- SEPP compatible with OCCNE1.2/1.3

Unified Data Manager (UDM)/Authentication Server Function (AUSF) Version 1.0.0

UDM/AUSF has been updated with the following enhancements:

- Deployable on Oracle Communications Cloud Native Environment (OCCNE) 1.3 and integrated to use DB Tier
- Integrated with CNE services
- Integrated with UDR(1.3) as backend data store
- Integrated with SCG as API gateway for ingress traffic
- Provides AUSF authentication capability as part of deployment
- Compliant with 29.503 v15.4.0
- Supports Nudm-ueau service for authentication procedures for 5G AKA
- Supports Nudm-uecm for context management procedures for AMF registrations, SMF registrations, SMSF for 3gpp access. Also supports implicit notifications to AMF

- Supports Nudm-sdm service for subscriber data management procedures for slice selection, AM, SM data

Unified Data Repository (UDR)/ Unstructured Data Storage Function (UDSF) Version 1.4.0

UDR/UDSF has been updated with the following enhancements:

- Support for Unified Data Manager (UDM) subscriptions and notifications

3

Oracle Communications Cloud Native Environment Alerts

This chapter provides information about the Oracle Communications Cloud Native Environment (OCCNE) alerts, and the alert rules used to implement them.

General Alerts

Alert Name	Summary	Description	Severity	Expression	For	SNMP Trap ID	Notes
SOFTWARE_INSTALLED	New software has been installed	{{ \$labels.product_name }} release {{ \$labels.engineering_release }} has been installed	info	software_deployment BY (engineering_release) == 0	N/A	1100	software_deployment metric values: 0 = installed 1 = upgrade in progress 2 = upgrade failed 3 = removed
UPGRADE_IN_PROGRESS	{{ \$labels.product_name }} is being upgraded	{{ \$labels.product_name }} is being upgraded to release {{ \$labels.engineering_release }}	info	software_deployment BY (engineering_release) == 1	N/A	1101	
UPGRADE_FAILED	{{ \$labels.product_name }} upgrade failed	{{ \$labels.product_name }} upgrade to release {{ \$labels.engineering_release }} failed	major	software_deployment BY (engineering_release) == 2	N/A	1102	
SOFTWARE_REMOVED	Software removed or replaced	{{ \$labels.product_name }} release {{ \$labels.engineering_release }} was removed	info	software_deployment BY (engineering_release) == 3	N/A	1103	This one needs to auto-clear after 2-3 days

Kubernetes Alerts

Alert Name	Alert Name	Alert Name	Alert Name	Alert Name	Alert Name	Alert Name	Alert Name
DISK_SPACE_LO W	Disk space is RUNNING OUT on node {{ \$labels.kubernetes_node }} for partition {{ \$labels.mountpoint }}	Disk space is almost RUNNING OUT for kubernetes node {{ \$labels.kubernetes_node }} for partition {{ \$labels.mountpoint }} (< 20% left)	critical	$((\text{node_filesystem_free_bytes} / \text{node_filesystem_size_bytes}) * 100) < 20$	1m	1001	software_deployment metric values: 0 = installed 1 = upgrade in progress 2 = upgrade failed 3 = removed
CPU_LOAD_HIGH	CPU load is high on host {{ \$labels.kubernetes_node }}	CPU load is high on host {{ \$labels.kubernetes_node }} CPU load {{ \$value }}% Instance : {{ \$labels.instance }}	warning	$\text{round}((1 - (\text{sum}(\text{node_cpu_seconds_total}\{\text{mode}=\text{"idle"}\}) \text{by} (\text{kubernetes_node}, \text{instance}) / \text{sum}(\text{node_cpu_seconds_total}) \text{by} (\text{kubernetes_node}, \text{instance}))) * 100, .01) > 80$	2m	1002	
LOW_MEMORY	Node {{ \$labels.kubernetes_node }} running out of memory	Node {{ \$labels.kubernetes_node }} available memory at {{ value }} percent	warning	$\text{avg BY} (\text{kubernetes_node}) (\text{avg_over_time}(\text{node_memory_MemAvailable}[10\text{m}])) / \text{avg BY} (\text{kubernetes_node}) (\text{avg_over_time}(\text{node_memory_MemTotal}[10\text{m}])) * 100 \leq 20$	1m	1007	

Alert Name	Alert Name	Alert Name	Alert Name	Alert Name	Alert Name	Alert Name	Alert Name
OUT_OF_MEMORY	Node {{ \$labels.kubernetes_node }} out of memory	Node {{ \$labels.kubernetes_node }} available memory at < 1 percent	critical	avg BY (kubernetes_node) (avg_over_time(node_memory_MemAvailable[1m])) / avg BY (kubernetes_node) (avg_over_time(node_memory_MemTotal[1m])) * 100 < 1	N/A	1008	Averaging over a smaller interval, and not requiring the OOM condition to persist, to get a more responsive alert. If the node has (almost) no free memory for 1 minute then we alert immediately.
NTP_SANITY_CHECK_FAILED	Clock not synchronized on node {{ \$labels.kubernetes_node }}	NTP service sanity check failed on node {{ \$labels.kubernetes_node }}	minor	node_timex_sync_status == 0	1m	1009	

Alert Name	Alert Name	Alert Name	Alert Name	Alert Name	Alert Name	Alert Name	Alert Name
NETWORK_UNAVAILABLE	Network interface {{ \$labels.device }} on node {{ \$labels.kubernetes_node }} is unavailable	Network interface {{ \$labels.device }} on node {{ \$labels.kubernetes_node }} is unavailable	critical	node_network_up(device=~"[eno eth].+") == 0	30s	1010	On bare metal, external network interfaces are assumed to start with the prefix "eno". On vCNE, they are assumed to start with "eth". Kubernetes creates lots of virtual network interfaces, some of which are always down, so we need to specifically select for these external-facing interfaces when alarming.
PVC_NEARLY_FULL	Persistent volume claim {{ \$labels.persistentvolumeclaim }} is nearly full	Persistent volume claim {{ \$labels.persistentvolumeclaim }} has {{ value }} % of allocated space remaining.	warning	(kubelet_volume_stats_available_bytes / kubelet_volume_stats_capacity_bytes) * 100 < 5	10m	1011	

Alert Name	Alert Name	Alert Name	Alert Name	Alert Name	Alert Name	Alert Name	Alert Name
PVC_FULL	Persistent volume claim {{ \$labels.persistentvolumeclaim }} is full	Persistent volume claim {{ \$labels.persistentvolumeclaim }} has {{ value }} % of allocated space remaining.	major	(kubelet_volume_stats_available_bytes / kubelet_volume_stats_capacity_bytes) * 100 < 0.1	10m	1012	
NODE_UNAVAILABLE	Kubernetes node {{ \$labels.node }} is unavailable	Kubernetes node {{ \$labels.node }} is not in Ready state	critical	kube_node_status_condition(condition="Ready", status="true") == 0	30s	1013	
ETCD_NODE_DOWN	Etd is down	Etd is not running or is otherwise unavailable	critical	sum(up(job=~".*etcd.*") == 1) == 0	30s	1014	

Common Service Alerts

Alert Name	Summary	Description	Severity	Expression	For	SNMP Trap ID	Notes
ELASTICSEARCH_CLUSTER_HEALTH_RED	Both primary and replica shards are not available	Instance {{ \$labels.instance }}: not all primary and replica shards are allocated in elasticsearch cluster {{ \$labels.cluster }}	critical	elasticsearch_cluster_health_statuses(color="red") == 1	1m	1003	

Alert Name	Summary	Description	Severity	Expression	For	SNMP Trap ID	Notes
ELASTICSEARCH_CLUSTER_HEALTH_YELLOW	The primary shard is allocated but replicas are not	Instance <code>{{ \$labels.instance }}</code> : not all primary and replica shards are allocated in <code>elasticsearch cluster {{ \$labels.cluster }}</code>	warning	<code>elasticsearch_cluster_health_statuses(color="yellow") == 1</code>	1m	1004	
ELASTICSEARCH_DOWN	Elasticsearch is down	Elasticsearch is not running or is otherwise unavailable	critical	<code>elasticsearch_cluster_health_up == 0</code>	10s	1016	
ELASTICSEARCH_TOO_FEW_DATA_NODES_RUNNING	<code>{{ \$labels.cluster }}</code> cluster running on less than 3 data nodes	There are only <code>{{ \$value }}</code> <code>elasticsearch data nodes running in {{ \$labels.cluster }}</code> cluster. Required number of data nodes are 3 or higher.	critical	<code>elasticsearch_cluster_health_number_of_data_nodes < 3</code>	2m	1005	

Alert Name	Summary	Description	Severity	Expression	For	SNMP Trap ID	Notes
FLUENTD_NOT_AVAILABLE	Fluentd is down	Fluentd is not running or is otherwise unavailable	critical	kube_daemonset_status_number_ready(daemonset="ocne-logs-fluentd-elasticsearch") == 0	10s	1015	Fluentd runs as a daemonset - i.e. one replica on each worker node. Unfortunately there is no easy way to track a replica failure to a specific worker node, plus the kube_pod_status_ready() metric seems to keep reporting on failed pods from the past, which would lead to false alerts. All we can do here is alert if all Fluentd replicas are down.
GRAFANA_DOWN	Grafana is down	Grafana is not running or is otherwise unavailable	major	up(app="grafana") == 0	30s	1024	
JAEGER_DOWN	Jaeger is down	Jaeger collector is not running or is otherwise unavailable	critical	kube_replicaset_status_ready_replicas(replicaset=~"ocne-tracer-jaeger-collector-.*") == 0	10s	1020	Reporting on the Jaeger collector only.

Alert Name	Summary	Description	Severity	Expression	For	SNMP Trap ID	Notes
KIBANA_DOWN	Kibana is down	Kibana is not running or is otherwise unavailable	major	<code>(kube_deployment_status_replicas_unavailable(deployment="ocne-kibana")) == kube_deployment_status_replicas_available(deployment="ocne-kibana")</code>	30s	1023	
METALLB_CONTROLLER_DOWN	The MetalLB controller is down	The MetalLB controller is not running or is otherwise unavailable	critical	<code>up(app="metallb", component="controller") == 0</code>	30s	1022	
METALLB_SPEAKER_DOWN	A MetalLB speaker is down	The MetalLB speaker on worker node <code>{{ \$labels.instance }}</code> is down	major	<code>up(app="metallb", component="speaker") == 0</code>	10s	1021	The up() metric doesn't tell us which worker node the MetalLB speaker was running on directly, but does give us the worker node IP.
PROMETHEUS_DOWN	Prometheus is down	Prometheus is not running or is otherwise unavailable	critical	<code>kube_deployment_status_replicas_available(deployment="ocne-prometheus-server") == 0</code>	10s	1017	
PROMETHEUS_NODE_EXPORTER_NOT_RUNNING	Prometheus Node Exporter is NOT running	Prometheus Node Exporter is NOT running on host <code>{{ \$labels.kubernetes_node }}</code>	critical	<code>up(app="prometheus-node-exporter") == 0</code>	1m	1006	
SNMP_NOTIFIER_DOWN	SNMP Notifier is down	SNMP Notifier is not running or is otherwise unavailable	critical	<code>kube_deployment_status_replicas_available(deployment="ocne-snmp-notifier") == 0</code>	10s	1019	

Node status alerts and alarms

Alert name	Summary	Severity	Expression	For	SNMP Trap ID	Notes
NODE_DOWN	MySQL {{ \$labels.node_type }} node having node id {{ \$labels.node_id }} is down	major	db_tier_data _node_status == 0	N/A	2001	A value of 0 is used to indicate that a node is down; 1 indicates that the node is up.

CPU alerts and alarms

Alert name	Summary	Severity	Expression	For	SNMP Trap ID	Notes
HIGH_CPU	Node ID {{ \$labels.node_id }} CPU utilization at {{ value }} percent.	warning	(100 - (avg(avg_ove r_time(db_t ier_cpu_os_i dle[10m])) BY (node_id))) >= 85	1m	2002	Alerting on average CPU utilization over the prior 10 minutes, rather than requiring the CPU utilization for every reporting period over a 10 minute interval to be > 85%.

Memory utilization alerts and alarms

Alert name	Summary	Severity	Expression	For	SNMP Trap ID	Notes
LOW_MEMORY	Node ID {{ \$labels.node_id }} memory utilization at {{ value }} percent.	warning	(avg_ove r_time(db_tier_ memory_use d_bytes[10m) BY (node_id, memory_typ e) / avg_ove r_time(db_tier_ memory_tota l_bytes[10m) BY (node_id, memory_typ e)) * 100 >= 85	1m	2003	Alerting on average memory utilization over the prior 10 minutes, rather than requiring the memory utilization for every reporting period over a 10 minute interval to be > 85%.

Alert name	Summary	Severity	Expression	For	SNMP Trap ID	Notes
OUT_OF_MEMORY	Node ID {{ \$labels.node_id }} out of memory.	critical	(db_tier_memory_used_bytes) BY (node_id, memory_type) >= (db_tier_memory_total_bytes) BY (node_id, memory_type)	N/A	2004	Any OOM condition should be alerted; no need for the condition to exist for a certain amount of time.

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

All components available for download from the Oracle Software Delivery Cloud (<https://edelivery.oracle.com/>) are in Table 4-1.

 **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 4-1 Media Pack Contents for Cloud Native Core 2.1.0

Part Number	Description
TBD	Oracle Communications Cloud Native Core Binding Support Function (BSF) 1.4.0
V984387-01	Oracle Communications Cloud Native Core Cloud Native Environment (CNE) 1.3.2.0.0
TBD	Oracle Communications Cloud Native Core Diameter Routing Agent (DRA) 1.4.0
TBD	Oracle Communications Cloud Native Core Inter-Working Function (IWF) 1.3.0
TBD	Oracle Communications Cloud Native Core Network Exposure Function (NEF) 1.2.0
TBD	Oracle Communications Cloud Native Core Network Repository Function (NRF) 1.4.0
TBD	Oracle Communications Cloud Native Core Network Slice Selection Function (NSSF) 1.2.0
TBD	Oracle Communications Cloud Native Core Policy and Charging Rules Function (PCRF) 1.4.0
TBD	Oracle Communications Cloud Native Core Policy Control Function (PCF) 1.4.0
TBD	Oracle Communications Cloud Native Core Service Communication Proxy (SCP) 1.4.0
TBD	Oracle Communications Cloud Native Core Security Edge Protection Policy (SEPP) 1.2.0
TBD	Oracle Communications Cloud Native Core Unified Data Repository (UDR) 1.4.0
V984388-01	Oracle Communications Cloud Native Core Unified Data Management (UDM) 1.0.0.0.0

Load Line Up for Cloud Native Core

Cloud Native Core Release 2.1.0 contains the following components:

Table 4-2 Load Line Up for Cloud Native Core

Components	Versions
Binding Support Function	1.4.0
Cloud Native Environment	1.3.2
Diameter Routing Agent	1.4.0
Inter-Working Function	1.3.0
Network Exposure Function	1.2.0
Network Repository Function	1.4.0
Network Slice Selection Function	1.2.0
Policy and Charging Rules Function	1.4.0
Policy Control Function	1.4.0
Security Edge Proxy Protection	1.2.0
Service Communication Proxy	1.4.0
Unified Data Repository	1.4.0
Unified Data Management	1.4.0

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
Binding Support Function
Binding Support Function (BSF) Installation Guide
Binding Support Function (BSF) User's Guide
Cloud Native Environment

Table 4-3 (Cont.) Documentation Pack Contents

CNE Installation Guide
CNE Custom Template
Diameter Routing Agent
Cloud Native Diameter Routing Agent (cnDRA) Installation Guide
cnDRA Custom Template
Inter-Working Function
Inter-Working Function (IWF) Installation Guide
Inter-Working Function (IWF) User's Guide
Inter-Working Function (IWF) Custom Template
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) Custom Template
Network Repository Function (NRF) User's Guide
Network Slice Selection Function
Network Slice Selection Function (NSSF) Installation Guide
Network Slice Selection Function (NSSF) Custom Template
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
Service Communication Proxy
Service Communication Proxy (SCP) Installation Guide
Service Communication Proxy (SCP) Custom Template
Service Communication Proxy (SCP) User's Guide
Security Edge Proxy Protection
Security Edge Proxy Protection (SEPP) Installation Guide
Security Edge Proxy Protection (SEPP) Custom Template
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
Unified Data Management (UDM) Custom Template

5

Resolved and Known Bugs

This chapter lists the resolved and known bugs for Cloud Native Core release 2.1.0.

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.

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 Resolved Bugs table lists bugs resolved in this release.

Table 5-1 CNE 1.3.2 Resolved Bugs

Bug Number	Severity	Found in Release	Title
OCCNE-1151	2	1.2.0	automatic db_deploy not working on icemark or delta_db
OCCNE-1274	2	1.3.0	retrieve_docker.sh templates are no longer in sync, and are broken
OCCNE-1296	2	1.2.0	PROVISION security playbook fails if http_proxy not defined
OCCNE-1304	2	1.2.0	Provision deployment of YUM update files due to out-of-scope variable use
OCCNE-1312	2	1.2.0	OCCNE k8 install fails due to networking issues
OCCNE-1405	2	1.3.0	OCCNE not supporting mixed gen8/gen9/gen10 groupings, or unexpected roles for hardware-type
OCCNE-1122	3	1.0.0	Missing target file for sed command at line 197 of occne-ks.cfg.j2
OCCNE-1222	3	1.2.0	k8s_install docker_images template hard-codes coredns image and version
OCCNE-1305	3	1.2.0	Provision installs KVM and does VM setup even if no DB or Bastion nodes are defined

Table 5-2 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 5-3 NRF 1.4.0 Resolved Bugs

Bug Number	Severity	Found in Release	Title
30141184	3	1.2.0	Host header in HTTP2 message is getting rejected and throwing exception by NRF

Table 5-4 PCRf 1.4.0 Resolved Bugs

Bug Number	Severity	Found in Release	Title
30775611	3	1.3.0	cnPCRf:1.3:Dynamic perf-core configuration required in UDR for success response for SNR/PUR/UDR

Table 5-5 SCP 1.4.0 Resolved Bugs

Bug Number	Severity	Found in Release	Title
30731754	3	1.2.3	VS optimized to maximize the accommodation of rules in a VS

Table 5-6 UDR/UDSF 1.4.0 Resolved Bugs

Bug Number	Severity	Found in Release	Title
OCUDR-482	3	1.3.0	SM Policy Data GET query field parameter SNSSAI format change
OCUDR-483	3	1.3.0	Notifications payload format change for PCF notifications
OCUDR-446	3	1.3.0	Content-type should be changed when UDR sends error response

Customer Known Bug List

Cloud Native Release 2.1, Customer Known Bugs table lists the known bugs and associated Customer Impact Statements. This information is provided for information purposes only.

Table 5-7 CNE 1.3.2 Customer Known Bugs

Bug Number	Severity	Found in Release	Title	Customer Impact
30761850	2	1.3.2	DB-Tier did not recover from post weekend Lab Shutdown	DB Tier requires manual procedure to recover from power disruption event.
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.

Table 5-7 (Cont.) CNE 1.3.2 Customer Known Bugs

Bug Number	Severity	Found in Release	Title	Customer Impact
30756164	3	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	3	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.
307766492	3	1.3.2	OCCNE-VCNE 1.3 — Need to Add VM Sizing/Openstack Flavor information to Installation Documentation	No customer impact. This doc bug is to add useful information to the customer facing documentation.
OCCNE-991	3	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.
OCCNE-1318	3	1.1.0	Add external IPs to SQL nodes (vCNE)	Cross-site replication will not function properly without external IPs. This is not an issue for applications not requiring replication to multiple sites.
OCCNE-1337	3	1.3.2	k8s install produces non-executable kubectll binary in ../artifacts	Minimal impact this only affects verification and diagnostic procedures.. There is a simple workaround that requires manual intervention.
OCCNE-1398	3	1.3.2	can't ssh to enclosure switches after configure from procedure.	Minimal impact since there is a simple workaround. Workaround: To ssh to OA then from OA "connect interconnect 1(1 for switch1 or 2 for switch2)" to access enclosure switches.
OCCNE-1464	3	1.2.1	OCCNE 1.2.0 Installation Guide Does Not Provide Guidance on Firmware Version	Installation procedure could fail if running on a server with older firmware.

Table 5-8 DRA 1.4.0 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 drawworker pod	1k connections could not be configured on drawworker pod.

Table 5-9 NRF 1.4.0 Customer Known Bugs

Bug Number	Severity	Found in Release	Title	Customer Impact
30736715	4	1.4.0	Primary MySql Host only considers 3306 Port value	Customer can only use default MySQL Port (3306)
30737221	4	1.4.0	NRF is not suspending UNDISCOVERABLE profiles if HB missed	No consumer NFs can ever know the when a UNDISCOVERABLE Profile becomes unavailable

Table 5-10 PCF 1.4.0 Customer Known Bugs

Bug Number	Severity	Found in Release	Title	Customer Impact
30776227	3	1.4	Binding data is not deleted, when we delete PDU session	
30776242	3	1.4	Unsubscribe of subscriber not happening towards UDR for AM Policy delete	
30776258	3	1.4	PCF1.3 version Rx interface will return duplicate AVPs in AAA reponse	
30776213	4	1.4	VPAT Issue in using keyboard for navigation using Policy Blocks	

Table 5-11 PCRF 1.4.0 Customer Known Bugs

Bug Number	Severity	Found in Release	Title	Customer Impact
30775276	2	1.3	cnPCRF:1.3: DB 'Too many connections' seen in pcrf-core log during performance testing	This Impacts the performance requirements. Workaround: None.
30775328	2	1.3	cnPCRF:1.3: CN-PCRF diam-gw support for Scaling of PCRF Core	This Impacts the scalability requirements. Workaround: You should restart Diameter Gateway after increasing the number of PCRF cores.
30775532	2	1.3	cnPCRF:1.3: Diam-gateway support for scaling of PCRF Core microservice	This Impacts the scalability requirements. Workaround: None.
30775308	2	1.3	cnPCRF 1.3: Policy action "Set session revalidation time to seconds" is not working	This impacts the functional requirement of event report after timer expiry. Workaround: None.

Table 5-12 SCP 1.4.0 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.
30731829	3	1.3	SCPC-Pilot is taking high CPU while applying updates if number of equivalent profiles/ ServiceInstances are exceeding 100	More CPU is consumed if updates are frequent. Workaround: To put pilot on a node where other processes are not consuming much of CPUs using node selector.

Table 5-12 (Cont.) SCP 1.4.0 Customer Known Bugs

Bug Number	Severity	Found in Release	Title	Customer Impact
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 5-13 UDM/AUSF 1.0.0 Customer Known Bugs

Bug Number	Severity	Found in Release	Title	Customer Impact
30542078	3	1.0.0	Encrypted authentication key support is not handled in UDM	The data stored on UDR is accessible for only UDM and hence minimal impact for customer/user.

Table 5-14 UDR/UDSF 1.4.0 Customer Known Bugs

Bug Number	Severity	Found in Release	Title	Customer Impact
OCUDR-463	3	1.4.0	Headers for few resources are not implemented as per spec 29505-v15.4.0	No impact. UDM(consumer of UDM APIs) does not send conditional attributes to UDR.
OCUDR-562	3	1.4.0	"changes" field value is missing in the notification payload	Notifications rate is limited in initial release.
OCUDR-563	3	1.4.0	UDR rejects sdmSubscription creation after deleting it when SubscriptionDataSub scription already exist	No impact.
OCUDR-418	4	1.3.0	UDR is not validating the conditional attributes for UDM APIs.	Affects when UDM does not cleanup subs-to-notify which is linked to sdmSubscriptions. Workaround: UDM needs to cleanup subs-to-notify and sdmSubscriptions mandatorily.

Table 5-14 (Cont.) UDR/UDSF 1.4.0 Customer Known Bugs

Bug Number	Severity	Found in Release	Title	Customer Impact
OCUDR-455	4	1.3.0	Notify Service delays notifications to PCF during traffic run	Affects only when multiple PATCH items are sent which triggers notifications. Workaround: You should not send delete and add in the same PATCH request.