

# Oracle® Communications

## Cloud Native Core Release Notes



Release 2.3.3

F40709-04

April 2021

ORACLE®

Copyright © 2019, 2021, Oracle and/or its affiliates.

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 embedded, installed or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software" or "commercial computer software documentation" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. 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 Inside 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, Epyc, and the AMD 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

---

## 2 Feature Descriptions

---

|   |     |
|---|-----|
| Binding Support Function (BSF)              | 2-1 |
| Cloud Native Environment (CNE)              | 2-1 |
| Cloud Native Diameter Routing Agent (CnDRA) | 2-2 |
| Cloud Native Core Console (CNC Console)     | 2-2 |
| CNC NF Data Collector                       | 2-2 |
| Cloud Native Core Policy (CNC Policy)       | 2-3 |
| Inter-Working Function (IWF)                | 2-3 |
| Service Communication Proxy (SCP)           | 2-4 |
| Security Edge Proxy Protection (SEPP)       | 2-4 |
| Network Exposure Function (NEF)             | 2-4 |
| Network Repository Function (NRF)           | 2-4 |
| Network Slice Selection Function (NSSF)     | 2-5 |
| Unified Data Management (UDM)               | 2-6 |
| Unified Data Repository (UDR)               | 2-6 |

## 3 Media and Documentation

---

|                                    |     |
|------------------------------------|-----|
| Media Pack                         | 3-1 |
| Security Certification Declaration | 3-6 |
| Documentation Pack                 | 3-7 |

## 4 Resolved and Known Bugs

---

|                         |     |
|-------------------------|-----|
| Severity Definitions    | 4-1 |
| Resolved Bug List       | 4-2 |
| Customer Known Bug List | 4-6 |

---

# 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:

- 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**.
- For Hardware, Networking and Solaris Operating System Support, select **3**.

You are connected to a live agent who can assist you with My Oracle Support registration and opening a support ticket.

My Oracle Support is available 24 hours a day, 7 days a week, 365 days a year.

# What's New In This Guide

This section introduces the documentation updates for Release 2.3.3 in Oracle Communications Cloud Native Core (CNC) Release Notes.

## **Release 2.3.3 - F40709-04, April 2021**

### **New and Updated Sections for NRF Release 1.11.1**

The following sections are updated for NRF Release 1.11.1:

- [Network Repository Function \(NRF\)](#): Added new feature/enhancement
- [Media Pack](#): Added Media pack details
- [Resolved Bug List](#): Added resolved bugs list

## **Release 2.3.3 - F40709-03, April 2021**

### **New and Updated Sections for SCP Release 1.11.0**

The following sections are updated for SCP Release 1.11.0:

- [Service Communication Proxy \(SCP\)](#): Added new feature/enhancement
- [Media Pack](#): Added Media pack details
- [Security Certification Declaration](#) : Added security certification declaration for SCP
- [Resolved Bug List](#): Added resolved bugs list
- [Customer Known Bug List](#): Added customer known bugs list

## **Release 2.3.3 - F40709-02, April 2021**

### **New and Updated Sections for CNC Console Release 1.6.1**

The following sections are updated for CNC Console Release 1.6.1:

- [Cloud Native Core Console \(CNC Console\)](#): Added new feature/enhancement
- [Customer Known Bug List](#): Added customer known bugs list
- [Media Pack](#): Added Media pack details

## **Release 2.3.3 - F40709-01, March 2021**

### **New and Updated Sections for BSF Release 1.8.0**

The following sections are updated for BSF Release 1.8.0:

- [Binding Support Function \(BSF\)](#): Added new features/enhancements
- [Media Pack](#): Added Media pack details

### **New and Updated Sections for CNC Console Release 1.6.0**

The following sections are updated for CNC Console Release 1.6.0:

- [Cloud Native Core Console \(CNC Console\)](#): Added new features/enhancements
- [Media Pack](#): Added Media pack details
- [Resolved Bug List](#): Added resolved bugs list

- 
- [Customer Known Bug List](#): Added customer known bugs list

#### **New and Updated Sections for CNC Policy Release 1.11.0**

The following sections are updated for CNC Policy Release 1.11.0:

- [Cloud Native Core Policy \(CNC Policy\)](#): Added new features/enhancements
- [Media Pack](#): Added Media pack details
- [Resolved Bug List](#): Added resolved bugs list
- [Customer Known Bug List](#): Added customer known bugs list

#### **New and Updated Sections for CNE Release 1.8.0**

The following sections are updated for CNE Release 1.8.0:

- [Cloud Native Environment \(CNE\)](#): Added new features/enhancements
- [Media Pack](#): Added Media pack details
- [Resolved Bug List](#): Added resolved bugs list
- [Customer Known Bug List](#): Added customer known bugs list

#### **New and Updated Sections for NRF Release 1.11.0**

The following sections are updated for NRF Release 1.11.0:

- [Network Repository Function \(NRF\)](#): Added new features/enhancements
- [Media Pack](#): Added Media pack details
- [Resolved Bug List](#): Added resolved bugs list
- [Customer Known Bug List](#): Added customer known bugs list

#### **New and Updated Sections for NSSF Release 1.5.0**

The following sections are updated for NSSF Release 1.5.0:

- [Network Slice Selection Function \(NSSF\)](#): Added new features/enhancements
- [Media Pack](#): Added Media pack details
- [Resolved Bug List](#): Added resolved bugs list
- [Customer Known Bug List](#): Added customer known bugs list

#### **New and Updated Sections for CNC UDR Release 1.11.0**

The following sections are updated for CNC UDR Release 1.11.0:

- [Unified Data Repository \(UDR\)](#): Added new features/enhancements
- [Media Pack](#): Added Media pack details
- [Resolved Bug List](#): Added resolved bugs list
- [Customer Known Bug List](#): Added customer known bugs list

# 1

## Introduction

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

# 2

## Feature Descriptions

This chapter provides a summary of each feature released in Cloud Native features release 2.3.3.

### Binding Support Function (BSF)

Binding Support Function (BSF) 1.8.0 has below enhancements:

- **Turning off AccessToken signature validation:** With this feature, CNC Binding Support Function has the capability to turn off AccessToken signature validation at the application layer. For instance, when service mesh, for example, Aspen Service Mesh, is integrated with BSF, the service mesh would perform the AccessToken validation. In such cases, the BSF shall skip validating AccessToken signature. For more information, see *Oracle Communications Cloud Native Core Binding Support Function Installation Guide*.
- **Alerts for change in Status of BSF and the Services:** New alerts are added to notify the operators on any change in BSF status and BSF services. For more information about these alerts, see *Oracle Communications Cloud Native Core Binding Support Function User's Guide*. **BSF\_Alertrules.yaml** file has also been updated as part of this feature. The **BSF\_Alertrules.yaml** file is packaged with BSF Custom Templates. The **BSF Custom Templates.zip** file can be downloaded from [MOS](#).

### Cloud Native Environment (CNE)

Cloud Native Environment (CNE) 1.8.0 provides the following major features in this release:

- **CNE Sizing and Performance - Common Services:** OCCNE allows the operator to perform predeployment sizing for persistent storage for metrics and logs. For more information, see *Oracle Communications Cloud Native Environment (OCCNE) Installation Guide* and *Oracle Communications Cloud Native Environment (OCCNE) Upgrade Guide*.
- **Bare Metal Redesign:** The new server and storage architecture is provided for baremetal deployments. The new baremetal architecture allows the cloud-native DBTier to be deployed on baremetal, and will eliminate issues affecting Prometheus and Elasticsearch during upgrade. It will also remove the special "storage servers" used by the DBTier, and replace them with an equal number of K8s worker nodes (making the minimum recommended deployment 6 worker nodes). For more information, see *Oracle Communications Cloud Native Environment (OCCNE) Installation Guide* and *Oracle Communications Cloud Native Environment (OCCNE) Upgrade Guide*.
- **Upgraded to Oracle Linux 8:** Both baremetal and virtualized CNE are using Oracle Linux 8. For more information, see *Oracle Communications Cloud Native Environment (OCCNE) Installation Guide* and *Oracle Communications Cloud Native Environment (OCCNE) Upgrade Guide*.



- **Cloud Native DBTier:** The cloud native DB Tier (cnDbTier) is a version of the DB Tier that runs entirely within Kubernetes, and uses Kubernetes persistent storage. For more information, see *cnDbTier Installation Guide* and *DBTier User Guide*.
- **DBTier 3-Site Replication:** This feature allows the users to replicate DBTier data to two other sites. Management of HA replication channels to both sites is automated, like in previous releases. 2-site replication is still supported as well. For more information, see *cnDbTier Installation Guide* and *DBTier User Guide*.

## Cloud Native Diameter Routing Agent (CnDRA)

There are no new features or updates implemented in CNC 2.3.3 release.

## Cloud Native Core Console (CNC Console)

Cloud Native Core Console (CNC Console) 1.6.1 has been updated with the following enhancement:

- **CNC Console GUI support for latest version of SCP (1.11.0):** CNC Console GUI is updated to support the latest version of SCP (1.11.0). For more information about the this, see *Oracle Communication Cloud Native Core Service Communication Proxy (SCP) Installation Guide* and *Oracle Communication Cloud Native Core Service Communication Proxy (SCP) User's Guide*.

Cloud Native Core Console (CNC Console) 1.6.0 has been updated with the following enhancements:

- **CNC Console Upgrade and Rollback support:** CNC Console IAM and CNC Console Core can be upgraded from the previous version to the current version using helm upgrade feature. For more information about the upgrade, see *Oracle Communications Cloud Native Core Console Installation and Upgrade Guide*.
- **Consistent Logging Screen for SCP, NRF, UDR:** Consistent Logging screens are supported for SCP, NRF and UDR. Policy and BSF already support Consistent Logging screens. For more information about the Consistent Logging screen, see *Oracle Communications Cloud Native Core Console User's Guide*.
- **CNC Console Metrics enhancements:** This enhancement supports security (Authentication and Authorization) related Metrics, KPIs, and Alerts. For more information about metrics, KPIs, and alerts, see *Oracle Communications Cloud Native Core Console User's Guide*.
- **Support latest version of NFs:** CNC Console 1.11.0 is compatible with latest version of already supported NFs:
  - SCP 1.11.0
  - NRF 1.11.0
  - UDR 1.11.0
  - CNC Policy 1.11.0
  - BSF 1.8.0

## CNC NF Data Collector

There are no new features or updates implemented in CNC 2.3.3 release.

## Cloud Native Core Policy (CNC Policy)

Oracle Communications Cloud Native Core Policy (CNC Policy) 1.11.0 has below enhancements:

- **PCF Interface Timer Handling Enhancements - Phase2:** The CNC Policy Solution now allows you to set request timeout values for **PCF Session Management** and **PCF UE Policy** services in applications/interfaces using timer profile. CNC Policy applies the specific timeout profile when sending a request to external NFs, the external NFs include UDR/CHF/NRF/BSF, and CNC Policy updates the appropriate metrics. For information on managing timer profile, see the Managing Timer Profile section in *Oracle Communications Cloud Native Core Policy User's Guide*.
- **Policy Table Enhancements - Phase 1:** The CNC Policy solution now allows you to modify the Key column values of a Policy Table. Also, new fields are introduced on the Policy Tables page to import, export, and clone a Policy Table. For information on managing policy tables, see the Managing Policy Tables section in *Oracle Communications Cloud Native Core Policy User's Guide*.
- **Policy Import/Export Enhancements - Phase 1:** With this enhancement, you can export policy table data using REST APIs. Also, this enhancement allows you to export individual policies and its dependencies using the REST APIs. For more information, see *Oracle Communications Cloud Native Core Policy REST API Guide*.
- **Diameter metrics enhancements - Phase 2:** With this enhancement, new Diameter Gateway Metrics have been added. For more information, see the Diameter Gateway Metrics section in *Oracle Communications Cloud Native Core Policy User's Guide*.
- **Manually Delete Session (phase II - deleting SMF, UDR, CHF):** With this enhancement, CNC Policy supports for request of termination of the SM association with the SMF which triggers SMF to delete the SM association, which will result in deleting associated contexts (e.g. UDR subscription, CHF, etc.). For more information, see *Oracle Communications Cloud Native Core Policy User's Guide*.
- **Handling of Install and Remove Conflict for Same Rule:** With this enhancement, when SM service receives two action types - install and remove for the same rule, SM service processes the remove action for the rule first, and then installs it. However, if install is not configured for the rule, SM service may remove it. For more information, see *Oracle Communications Cloud Native Core Policy User's Guide*.
- **Alerts for change in Status of PCF and the Services:** New alerts are added to notify the operators on any change in PCF status and PCF services. For more information about these alerts, see *Oracle Communications Cloud Native Core Policy User's Guide*. **PCF\_Alertrules.yaml** has also been updated as part of this feature. The **PCF\_Alertrules.yaml** file is packaged with CNC policy Custom Templates. The **CNC Policy Custom Templates.zip** file can be downloaded from [MOS](#).

## Inter-Working Function (IWF)

There are no new features or updates implemented in CNC 2.3.3 release.

## Service Communication Proxy (SCP)

SCP 1.11.0 has been updated with the following enhancements:

- **Ingress Rate Limiting Support:** SCP secures the network when aggregated ingress traffic from an NF instance exceeds the allowed limit. If the traffic exceeds the allowed limit, SCP does not process the traffic and responds with an error code. For more information about the feature, see *Oracle Communications Cloud Native Core Service Communication Proxy (SCP) User's Guide*.
- **Egress Rate Limiting Support:** The Egress Rate Limiting feature stops the producer NF instance from getting overloaded. SCP secures the network when aggregated egress traffic from any registered NF instance exceeds the allowed limit. If the traffic exceeds the allowed limit, SCP performs the alternate routing by default. In case alternate routing is not configured, SCP responds with an error code. For more information about the feature, see *Oracle Communications Cloud Native Core Service Communication Proxy (SCP) User's Guide*.
- **REST APIs to support Helm based configurations changes runtime:** SCP supports updating Helm configurable options after deployment using REST API parameters. For more information about the feature, see *Oracle Communications Cloud Native Core Service Communication Proxy (SCP) User's Guide*.
- **NRF Preventive Audit check:** SCP controls NRF failure scenarios in the network by performing the preventive audit (discovery). This audit is performed with all the configured regional NRFs before removing the last NF instance of a particular NF type. For more information about the feature, see *Oracle Communications Cloud Native Core Service Communication Proxy (SCP) User's Guide*.
- **Not consider Serving Scope while calculating profile hash:** SCP is optimized Audit and Notification to not consider serving scope while hash calculation. For more information about the feature, see *Oracle Communications Cloud Native Core Service Communication Proxy (SCP) Installation Guide*.

## Security Edge Proxy Protection (SEPP)

There are no new features or updates implemented in CNC 2.3.3 release.

## Network Exposure Function (NEF)

There are no new features or updates implemented in CNC 2.3.3 release.

## Network Repository Function (NRF)

OCNRF 1.11.1 has been updated with the following enhancement:

- **Enabling OAuth2 Token caching at OCNRF:** OCNRF supports catching of OAuth2 token for SLF communication at OCNRF. For more information about this feature, see *Oracle Communications Cloud Native Core NRF User's Guide*.

OCNRF 1.11.0 has been updated with the following enhancements:

- **Alerts for change in NF Status and NF Service Status at NRF:** New alerts are added to notify the operators on any change in NF status and NF services. For

more information about these alerts, see *Oracle Communications Cloud Native Core NRF User's Guide*.

- **Support for configurable Primary/Secondary/Tertiary Locality for Locality based Discovery response:** OCNRF Extended Preferred Locality Priority Handling feature allows the operator to set priority of NF profiles in response of 3GPP defined NFDISCOVER service operation of NRF. For more information about Extended Preferred Locality Priority Handling feature, see *Oracle Communications Cloud Native Core NRF User's Guide*.
- **CNC Console support for configuring Key details for AccessToken:** Key-ID feature allows the operator to add "kid" header in Access Token Response generated by OCNRF. OCNRF allows configuring KeyID using CNC Console. For more information about configuring KeyID, see *Oracle Communications Cloud Native Core NRF Installation and Upgrade Guide*.
- **Automation of Control Plane Configuration using Helm Chart:** With this enhancement, the control plane configuration can be done at the time of OCNRF installation using helm chart. For more information, see *Oracle Communications Cloud Native Core Network Repository Functions (NRF) Installation and Upgrade Guide*.
- **Support for Dynamic Logging for all micro-services using REST/CNCC:** OCNRF allows the operator to change the log level of individual services dynamically (without POD restart). It also allows the operator to retrieve the current log level of all the services. This feature can be configured using REST API or CNC Console. For more information, see *Oracle Communications Cloud Native Core Network Repository Functions (NRF) User's Guide*.
- **Support for Per NF Type Alert for Active Registered NFs:** OCNRF allows to configure the alerts for a specific type of NF. It also allows to configure the threshold value per NF. For more information, see *Oracle Communications Cloud Native Core Network Repository Functions (NRF) User's Guide*.

## Network Slice Selection Function (NSSF)

OCNSSF 1.5.0 has been updated with the following enhancements:

- **Support for multiple PLMN at NSSF:** This feature enables single NSSF instance to cater to multiple PLMNs. This enables operator to define slice selection policies for multiple PLMNs, and gives the option for operator to span a network slice across PLMNs. For more information about this feature, see *Oracle Communications Cloud Native Core Network Slice Selection Function (NSSF) User's Guide*.
- **Two site GR Support for NSSF :** OCNSSF supports two site georedundancy to ensure service availability when one OCNSSF site is down. For more information on this feature, see *Oracle Communications Cloud Native Core Network Slice Selection Function (NSSF) User's Guide*.
- **Integrated Debug tool:** Debug tool provides third-party troubleshooting tools for debugging the runtime issues for lab and production environment. For more information on the usage of this tool, see *Cloud Native Core Network Slice Selection Function (NSSF) Installation Guide*.
- **Supports Integration with ASM:** With this enhancement, the ASM configures automatically at the time of NSSF installation. For more information on the usage of this tool, see *Cloud Native Core Network Slice Selection Function (NSSF) Installation Guide*.

- **Dynamic log level update:** Common Configuration Service lets OCNSSF centralize its configuration and update it dynamically without a restart. For more information, see the Runtime Log Level Update section of the *Oracle Communications Cloud Native Core Network Slice Selection Function (NSSF) User's Guide*.
- **ATS support:** OCNSSF supports Automated Testing Suite for validating the functionalities. Georedundancy and Multiple PLMN are part of NSSF new features pipeline. Jenkins plugin of Test Result Analyzer is also added. For more information, see *Oracle Communications Cloud Native Core Automated Test Suite (ATS) Guide*.

## Unified Data Management (UDM)

There are no new features or updates implemented in CNC 2.3.3 release.

## Unified Data Repository (UDR)

UDR 1.11.0 has been updated with the following enhancements:

- **Automated ASM configurations during NF installation:** With this enhancement, the ASM configures automatically at the time of UDR installation. For more information, see Chapter 4 - ASM Data Plane Configuration using Helm of the *Oracle Communications Cloud Native Core Unified Data Repository Installation and Upgrade Guide*.
- **Enhancements to Helm install (Automatic DB creation):** The UDR database user, password and granting of permissions to the user are currently manual action as part of the UDR Installation. With this enhancement, the operator can install UDR via Helm and all these manual operations are automated. For more information, see the Planning Your Installation section of Chapter 2, Installing Unified Data Repository in the *Oracle Communications Cloud Native Core Unified Data Repository Installation and Upgrade Guide*.
- **Support of XFCC header at SLF:** With this enhancement, UDR/SLF supports XFCC header validation for the ingress traffic that originates via SCP. It provides a way to validate the origin SCP from which requests are received on UDR/SLF. For more information, see the Configuring User Parameters section of the *Oracle Communications Cloud Native Core Unified Data Repository Installation and Upgrade Guide*.
- **Common Config Service APIs Integration:** With this enhancement, common services like Ingress Gateway, Egress Gateway, Alternate Route Service are now configurable using REST based APIs. For more information, see *Oracle Communications Cloud Native Core Unified Data Repository REST Specification Guide*.
- **Logging and Tracing Improvements for UDR:** With this enhancement, UDR logging level and tracing practices are improved. For more information, see Understanding Log Attribute Details section of the *Oracle Communications Cloud Native Core Unified Data Repository Installation and Upgrade Guide*.
- **Logging and Tracing Improvements for Provisioning Gateway:** With this enhancement, Provisioning Gateway logging level and tracing practices are improved. For more information, see Understanding Log Attribute Details section of the *Oracle Communications Cloud Native Core Provisioning Gateway Guide*.

- **Addition of Non-SLF Features to UDR ATS:** With this release, Non-SLF features like policy data, udm data, diameter etc are added to UDR ATS. For more information, see *Oracle Communications Automated Testing Suite Guide*.

# 3

## Media and Documentation

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

### Media Pack

This section lists the media package for Cloud Native Core 2.3.3. For downloading the package, refer to [MOS](#).

#### Note:

This list is accurate at the time of release but is subject to change. See the Oracle software delivery website for the latest information.

**Table 3-1 Media Pack Contents for Cloud Native Core 2.3.3**

| Description   | Versions | ATS Test Cases Included | Upgrade  | Compliance   |
|---|----------|-------------------------|--|--|
| Oracle Communications Cloud Native Core Console (CNCC)                | 1.6.1    | NA                      | <ul style="list-style-type: none"> <li>Upgrade from CNCC 1.5.x to 1.6.x is supported</li> <li>Upgrade from CNCC 1.6.0 to 1.6.1 is supported</li> </ul> | Compatible with: <ul style="list-style-type: none"> <li>SCP 1.11.0</li> <li>NRF 1.11.0</li> <li>UDR 1.11.0</li> <li>Policy 1.11.0</li> <li>BSF 1.8.0</li> <li>CNDBTier 1.8.0</li> <li>OSO 1.6.2</li> <li>ASM 1.5.7-am3 and ASM 1.4.6-am9</li> <li>CNE 1.8.0, CNE 1.7.x, and CNE 1.6.0</li> </ul> |
| Oracle Communications Cloud Native Core Automated Testing Suite (ATS) | 1.6.0    | NA                      | Supports fresh installation only   | Compatible with: <ul style="list-style-type: none"> <li>CNE 1.6.0 and CNE 1.7.0</li> </ul>   |

Table 3-1 (Cont.) Media Pack Contents for Cloud Native Core 2.3.3

| Description  | Versions | ATS Test Cases Included   | Upgrade   | Compliance   |
|--|----------|---|---|--|
| Oracle Communications Cloud Native Core Binding Support Function (BSF) | 1.8.0    | Yes<br><br><b>Note:</b> Not applicable to: <ul style="list-style-type: none"> <li>Support for Debug Tool</li> <li>Consistent Logging Level Support</li> </ul> | BSF 1.8.0 supports fresh installation as well as upgrade from 1.7.x to 1.8.0.<br><br>For more information on installation/upgrading, see <i>Oracle Communications Cloud Native Core Binding Support Function Installation and Upgrade Guide</i> | Compatible with: <ul style="list-style-type: none"> <li>NRF 1.11.0</li> <li>UDR 1.11.0</li> <li>CNC Policy 1.11.0</li> <li>CNDBTier 1.8.0</li> <li>OSO 1.6.1 and 1.7.0</li> <li>ASM 1.5.10</li> <li>CNE 1.7.0 and CNE 1.6.0</li> </ul>   |
| Oracle Communications Cloud Native Core Console (CNCC)                 | 1.6.0    | NA  | Upgrade from CNCC 1.5.x to 1.6.0 is supported   | Compatible with: <ul style="list-style-type: none"> <li>SCP 1.11.0</li> <li>NRF 1.11.0</li> <li>UDR 1.11.0</li> <li>Policy 1.11.0</li> <li>BSF 1.8.0</li> <li>CNDBTier 1.8.0</li> <li>OSO 1.6.2</li> <li>ASM 1.5.7-am3 and ASM 1.4.6-am9</li> <li>CNE 1.8.0, CNE 1.7.x, and CNE 1.6.0</li> </ul> |
| Oracle Communications Cloud Native Core Cloud Native Environment (CNE) | 1.8.0    | NA  | Upgrade supported from OCCNE 1.5.0 to OCCNE 1.6.0.<br><br>For more information, refer the <i>CNE Upgrade Guide</i> .  | NA   |



Table 3-1 (Cont.) Media Pack Contents for Cloud Native Core 2.3.3

| Description   | Versions | ATS Test Cases Included   | Upgrade   | Compliance   |
|---|----------|---|---|--|
| Oracle Communications Cloud Native Core Policy (CNC Policy)             | 1.11.0   | Yes<br><br><b>Note:</b> Not applicable to: <ul style="list-style-type: none"> <li>Support for Debug Tool</li> <li>Session Viewer REST API support for GET and DELETE</li> </ul> | CNC Policy 1.11.0 supports fresh installation as well as upgrade from 1.10.x to 1.11.0.<br><br>For more information on installation/upgrading, see <i>Oracle Communications Cloud Native Core Policy Installation and Upgrade Guide</i> | Compatible with: <ul style="list-style-type: none"> <li>NRF 1.11.0</li> <li>UDR 1.11.0</li> <li>BSF 1.8.0</li> <li>CNDBTier 1.8.0</li> <li>OSO 1.6.1 and 1.7.0</li> <li>ASM 1.5.10</li> <li>CNE 1.7.0 and CNE 1.6.0</li> </ul> |
| Oracle Communications Cloud Native Core Diameter Routing Agent (CnDRA)  | 1.6.0    | NA  | Supports fresh installation only  | NA   |
| Oracle Communications Cloud Native Core Inter-Working Function (IWF)    | 1.5.0    | NA  | Supports fresh installation only  | Compatible with: <ul style="list-style-type: none"> <li>BSF 1.5.0</li> <li>NRF 1.7.0</li> <li>UDR 1.7.0</li> <li>Compliant with 3GPP version 15.5</li> </ul>   |
| Oracle Communications Cloud Native Core Network Exposure Function (NEF) | 1.2.0    | NA  | Supports fresh installation only  | NA   |

Table 3-1 (Cont.) Media Pack Contents for Cloud Native Core 2.3.3

| Description   | Versions | ATS Test Cases Included | Upgrade   | Compliance  |
|---|----------|-------------------------|---|---|
| Oracle Communications Cloud Native Core Network Repository Function (NRF) | 1.11.1   | Yes                     | OCNRF 1.11.1 supports fresh installation. Also, supports upgrade from 1.10.x to 1.11.1 and 1.11.0 to 1.11.1. For more information about installation/upgrading, see <i>Oracle Communications Cloud Native Core NRF Installation and Upgrade Guide</i> . | Compatible with: <ul style="list-style-type: none"><li>• UDR 1.11.0</li><li>• CNDBTier 1.8.0.0.3 (with and without ASM)</li><li>• OSO 1.6.2</li><li>• ASM 1.5.10-am2</li><li>• OCCNE 1.7.0</li><li>• Network functions which are compliant with 3GPP Release: 29.510 v15.5 (September 2019) and 29.510 v16.3<ul style="list-style-type: none"><li>– Support for NFSet parameter</li><li>– Support for SCP as NfType</li></ul></li></ul> |

Table 3-1 (Cont.) Media Pack Contents for Cloud Native Core 2.3.3

| Description   | Versions | ATS Test Cases Included | Upgrade   | Compliance  |
|---|----------|-------------------------|---|---|
| Oracle Communications Cloud Native Core Network Repository Function (NRF)       | 1.11.0   | Yes                     | OCNRF 1.11.0 supports fresh installation as well as upgrade from 1.10.x to 1.11.0. For more information about installation/upgrading, see <i>Oracle Communications Cloud Native Core NRF Installation and Upgrade Guide</i> . | Compatible with: <ul style="list-style-type: none"> <li>• UDR 1.11.0</li> <li>• CNDBTier 1.8.0.0.3 (with and without ASM)</li> <li>• OSO 1.6.2</li> <li>• ASM 1.5.10-am2</li> <li>• OCCNE 1.7.0</li> <li>• Network functions which are compliant with 3GPP Release: 29.510 v15.5 (September 2019) and 29.510 v16.3 <ul style="list-style-type: none"> <li>– Support for NFSet parameter</li> <li>– Support for SCP as NfType</li> </ul> </li> </ul> |
| Oracle Communications Cloud Native Core Network Slice Selection Function (NSSF) | 1.5.0    | NA                      | Supports fresh installation only  | Compatible with: <ul style="list-style-type: none"> <li>• CNE 1.7.x</li> <li>• cnDBTier 1.7.x</li> <li>• OSO 1.6.2</li> <li>• ASM 1.5.7-am3</li> </ul>  |
| Oracle Communications Cloud Native Core Service Communication Proxy (SCP)       | 1.11.0   | Yes                     | Supports fresh installation only  | Compatible with CNE 1.6.0, CNE 1.7.0, CNE 1.8.0, OSO 1.6, CnDBTier 1.8.0 and ASM 1.5.10-am2   |

**Table 3-1 (Cont.) Media Pack Contents for Cloud Native Core 2.3.3**

| Description  | Versions | ATS Test Cases Included   | Upgrade   | Compliance   |
|--|----------|---|---|--|
| Oracle Communications Cloud Native Core Security Edge Protection Policy (SEPP) | 1.4.1    | Yes<br><br><b>Note:</b> Not applicable to: <ul style="list-style-type: none"> <li>Logging</li> <li>Alerts</li> <li>Metrics</li> </ul> | Supports fresh installation as well as upgrade from 1.4.0 to 1.4.1.<br><br>For more information on installation or upgrading, see <i>Oracle Communications Cloud Native Core Security Edge Protection Proxy (SEPP) Installation Guide</i> . | NA   |
| Oracle Communications Cloud Native Core Unified Data Repository (UDR)          | 1.11.0   | Yes   | UDR 1.11.0 supports fresh installation as well as upgrade from 1.10.x to 1.11.0.<br><br>For more information on installation/upgrading, see <i>Cloud Native United Data Repository Installation and Upgrade Guide</i> .                     | Compatible with <ul style="list-style-type: none"> <li>CNE 1.6.0 and CNE 1.7.0</li> <li>cnDBTier 1.6.0.0.0, 1.8.0.0.1, 1.8.0.0.3</li> <li>OSO 1.6.x</li> <li>ASM 1.5.10-am2</li> </ul> |
| Oracle Communications Cloud Native Core Unified Data Management (UDM)          | 1.1.0    | NA  | Supports fresh installation only  | NA   |

## Security Certification Declaration

The following table lists the security tests and the corresponding dates of compliance for each network function.

**Table 3-2 Security Certification Declaration**

| Compliance Test Description                      | BSF            | CNC Consol e   | CNC Policy     | CNE | NRF                          | NSSF | SCP | UDR                          |
|--|----------------|----------------|----------------|-----|------------------------------|------|-----|------------------------------|
| Systems test on functional and security features | March 18, 2021 | March 12, 2021 | March 18, 2021 | NA  | NA (no new security feature) | NA   | NA  | NA (no new security feature) |

**Table 3-2 (Cont.) Security Certification Declaration**

| <b>Compliance Test Description</b>           | <b>BSF</b>     | <b>CNC Console</b> | <b>CNC Policy</b> | <b>CNE</b>     | <b>NRF</b>     | <b>NSSF</b>    | <b>SCP</b>     | <b>UDR</b>     |
|--|----------------|--------------------|-------------------|----------------|----------------|----------------|----------------|----------------|
| Regression testing on security configuration | March 18, 2021 | March 12, 2021     | March 18, 2021    | March 18, 2021 | March 12, 2021 | NA             | NA             | March 12, 2021 |
| Vulnerability testing                        | March 15, 2021 | March 12, 2021     | March 12, 2021    | March 18, 2021 | March 10, 2021 | March 12, 2021 | April 01, 2021 | March 11, 2021 |
| Fuzz testing on external interfaces          | March 05, 2021 | February 24, 2021  | March 05, 2021    | March 18, 2021 | March 12, 2021 | March 12, 2021 | March 26, 2021 | March 12, 2021 |

## Documentation Pack

All documents are available for download from the [MOS](#) site.

# 4

## Resolved and Known Bugs

This chapter lists the resolved and known bugs for Cloud Native Core release 2.3.2.

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

### Severity Definitions

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

#### Severity 1

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

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

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

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

#### Severity 2

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

**Severity 3**

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

**Severity 4**

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

## Resolved Bug List

The following Resolved Bugs tables list the bugs that are resolved in Cloud Native Release 2.3.3.

**Table 4-1 CNC Console 1.6.0 Resolved Bugs**

| Bug Number | Severity | Found in Release | Title   |
|------------|----------|------------------|---|
| 32611157   | Minor    | 1.5.0            | CNCC 1.5: ASM integration to wait for istio-proxy sidecar before executing application code |
| 32151129   | Minor    | 1.4.0            | CNCC 1.4 : Policy bulk import screen progress bar is not getting updated                    |
| 32291243   | Minor    | 1.5.0            | CNCC - OCCNE 1.7.0 Kibana API prefix is not working   |
| 32291262   | Minor    | 1.5.0            | CNCC : Disable Grafana login screen   |
| 32641844   | Minor    | 1.5.2            | VZW CNCC - Request to Change the Name of Alert Rules File                                   |

**Table 4-2 CNC Policy 1.11.0 Resolved Bugs**

| Bug Number | Severity | Found in Release | Title  |
|------------|----------|------------------|--|
| 32377213   | 3        | 1.8.0            | Diameter connector to sm-service timer is hard coded to 2 sec                                |
| 32377250   | 3        | 1.10.0           | PCRF-Core should request to delete subscriber info from Policy-ds when subscriber detach     |
| 32388565   | 3        | 1.10.0           | SM Service Memory Growth during ATS run  |
| 32388574   | 3        | 1.10.0           | Audit Service getting hanged and thus not auditing the records                               |
| 32388591   | 3        | 1.10.0           | "udrconnector.apiroot" environment variable missing during helm upgrade from 1.9.1 to 1.10.0 |
| 32388592   | 3        | 1.10.0           | SM Service getting hanged with 10 K TPS  |

**Table 4-2 (Cont.) CNC Policy 1.11.0 Resolved Bugs**

| Bug Number | Severity | Found in Release | Title  |
|------------|----------|------------------|--|
| 32388606   | 3        | 1.10.0           | Egress GW Internal Server Error while sending Notify Request (N7 Notification) |
| 32388607   | 3        | 1.10.0           | PCF Session Binding Issue in SM Service (Null Pointer Exception)               |

**Table 4-3 CNE 1.8.0 Resolved Bugs**

| Bug Number | Severity | Found in Release | Title  |
|------------|----------|------------------|--|
| OCCNE-2425 | 2        | 1.4.0            | ES data not deleted when PV full   |
| OCCNE-3896 | 2        | 1.8.0            | OC-CNE 1.8 GA build fails  |
| OCCNE-3751 | 2        | 1.7.0            | Checking the status of the replication and switching the replication channel   |
| OCCNE-3758 | 2        | 1.8.0            | 1.8 rc.1 Failure to install on BM with no CNDBTIER selected  |
| OCCNE-3875 | 3        | 1.8.0            | db-backup-executor-svc logs username/password  |
| OCCNE-3876 | 3        | 1.8.0            | cndbtier cross site replication does not work using loadbalancer ip in vCNE  |
| OCCNE-3752 | 3        | 1.8.0            | Upgrade fails for Elasticsearch Data   |
| OCCNE-3810 | 3        | 1.8.0            | lbvm ip rule/route is missing after some service created   |
| OCCNE-3769 | 3        | 1.8.0            | vCNE Openstack (at least) need to set MTU appropriately to communicate with cloud-provider                                   |
| OCCNE-3803 | 3        | 1.8.0            | cnDbTier fails to deploy in OCI environment  |
| OCCNE-3802 | 3        | 1.8.0            | haproxy_handler.py script creates haproxy configuration with error messages on lbvm which results in haproxy service failure |
| OCCNE-3766 | 3        | 1.8.0            | Services exist from kubect! command, but failed for lookup lb-apiserver.kubernetes.local                                     |
| OCCNE-3756 | 3        | 1.8.0            | lbvm interfaces for haproxy are missing for ol8  |
| OCCNE-3745 | 3        | 1.8.0            | Upgrade fails for Grafana and Prometheus   |
| OCCNE-3759 | 3        | 1.8.0            | 1.8 rc.1 Loadbalancer services are not assigned with ip address  |
| OCCNE-2932 | 3        | 1.5.0,1.6.0      | Openstack certificate not passed during upgrade results in upgrade failure during k8s stage                                  |
| OCCNE-3455 | 3        | 1.6.0            | Get Scanning working on clusters with multiple bastions  |



Table 4-3 (Cont.) CNE 1.8.0 Resolved Bugs

| Bug Number | Severity | Found in Release | Title  |
|------------|----------|------------------|--|
| OCCNE-3861 | 4        | 1.8.0            | db-backup-manager-svc runs as a user other than mysql (27)   |
| OCCNE-3711 | 4        | 1.7.0            | kubectrl top command failing   |
| OCCNE-3585 | 4        | 1.6.0            | DBTier 1.8.0.0.1 CSAR descriptor_version value is not set to the software version in vnfd.yml file |
| OCCNE-3414 | 4        | 1.6.0            | cndbtier deployment occasionally fails to create all mysql users                                   |
| OCCNE-3760 | 4        | 1.7.0, 1.8.0     | Implement resource limits on jaeger components   |
| OCCNE-2543 | 4        | 1.4.0            | The /etc/hosts names have duplicate names and additional very long names                           |
| OCCNE-1337 | 4        | 1.2.0            | k8s_install produces non-executable kubectrl binary in ../artifacts                                |
| OCCNE-3528 | 4        | 1.7.0, 1.8.0     | Kibana default API Prefix in not working in CNCC setup for common services hyperlinks              |
| OCCNE-3744 | 4        | 1.7.0, 1.8.0     | Unable to drain worker nodes that host Istio pods  |
| OCCNE-3532 | 4        | 1.7.0            | Some of the OCCNE alert rules are not logically correct  |
| OCCNE-3531 | 4        | 1.7.0            | GRAFANA_DOWN alert not working   |
| OCCNE-3345 | 4        | 1.6.0            | k8s cannot verify user is non-root for db-monitor-svc and db-replication-svc                       |

Table 4-4 NRF 1.11.1 Resolved Bugs

| Bug Number | Severity | Found in Release | Title  | Customer Impact  |
|------------|----------|------------------|--|--|
| 32751028   | 3        | 1.11.0           | App-Info restarts continuously due to probe failure      | While Deploying NRF, CPU of AppInfo micro-service needs to be increased                                  |
| 32751034   | 4        | 1.11.0           | Alert file in the CSAR package needs to have static name | If Orchestrator's expects that the Alert Rule fine name needs to be a static name, then loading may fail |

Table 4-4 (Cont.) NRF 1.11.1 Resolved Bugs

| Bug Number | Severity | Found in Release | Title  | Customer Impact   |
|------------|----------|------------------|--|---|
| 32751048   | 4        | 1.11.0           | IGW's Cache service should not get assigned with LB IP | LB IP will get assigned to a non LB service if Operator uses Service section of IGW for assigning External LB annotations |

Table 4-5 NRF 1.11.0 Resolved Bugs

| Bug Number | Severity | Found in Release | Title  |
|------------|----------|------------------|--|
| 32623131   | 3        | 1.8.0            | NRF is replacing an incorrect FQDN in PATCH request when FQDN header validation is enabled |
| 32365728   | 3        | 1.10.0           | OCNRF's Host scheme can not be changed to HTTPs  |
| 32365433   | 4        | 1.10.0           | Invalid SupiRange is accepted during NFs Registering with NRF                              |
| 32365453   | 4        | 1.10.0           | Invalid Identity Range is accepted during NFs Registering with NRF                         |
| 32623138   | 4        | 1.10.0           | AccessToken-svc is non-responsive for requests with empty/invalid request body             |
| 32623151   | 3        | 1.10.0           | NFSetId Support - Access Token Claims don't support producerNfSetId                        |

Table 4-6 SCP 1.11.0 Resolved Bugs

| Bug Number | Severity | Found in Release | Title   |
|------------|----------|------------------|---|
| 32653951   | 2        | 1.9.1            | AuditMaster thread is getting killed during DB exception                                    |
| 32653962   | 3        | 1.10.0           | SCP worker is crashing in handling inter-SCP case with location uri with relative URI       |
| 32653968   | 3        | 1.10.0           | Log message to be included with exception stacktrace  |
| 32680387   | 3        | 1.10.1           | SCP worker throws recursive call error in log with more response time for incoming messages |
| 32653111   | 3        | 1.10.0           | Update InterSCP Audit testcase to avoid race condition between notification and audit       |

**Table 4-6 (Cont.) SCP 1.11.0 Resolved Bugs**

| Bug Number | Severity | Found in Release | Title   |
|------------|----------|------------------|---|
| 32653117   | 3        | 1.10.0           | Update Default SCP response timeout and Increase stub resources in ATS                |
| 32653129   | 3        | 1.10.0           | Enhance ATS to retry on stub connection Errors  |
| 32699327   | 4        | 1.9.1            | Different log level shows for the same log  |
| 32714175   | 4        | 1.10.0           | VZW SCP - API specification document (Swagger or YAML) for SCP configuration services |
| 32714191   | 4        | 1.9.0            | Change the name of Alert rules file in future releases in CSAR package                |
| 32714230   | 4        | 1.10.0           | The 5G (SCP) ATS Stubs should be helm deployable and stay static                      |

**Table 4-7 UDR 1.11.0 Resolved Bugs**

| Bug Number | Severity | Found in Release | Title   | Notes  |
|------------|----------|------------------|---|--|
| 32377421   | 3        | 1.10.0           | nudr-config PUT request for DR-SERVICE fails with the error Internal Server Error           | Occurs only when on-demand migration is enabled. |
| 32377299   | 4        | 1.10.0           | Duplicate key entries in the database for PUR requests                                      | Occurs only when auto-enrolment is enabled.      |
| 32377325   | 4        | 1.10.0           | subscription request fails with the error `Data field does not exist for Custom APIs        | NA   |
| 32377407   | 4        | 1.10.0           | UDM SDM subscription PATCH giving Invalid data content instead of Schema validation failure | NA   |

## Customer Known Bug List

Customer Known Bugs tables list the known bugs and associated Customer Impact Statements. This information is provided for information purposes only.

**Table 4-8 CNC Console 1.6.0 and 1.6.1 Customer Known Bugs**

| Bug Number | Severity | Found in Release | Title  | Customer Impact  |
|------------|----------|------------------|--|--|
| 31355530   | Minor    | 1.1.0            | CNCC IAM - Unable to remove assigned User Role                             | User will be able to add roles but user will not be able to remove the assigned roles.<br><b>Workaround:</b> Delete user and recreate user with required role.   |
| 32291223   | Minor    | 1.5.0            | CNCC : CNE Common Services type should be ClusterIP when accessed via CNCC | User will be able to access CNE common services directly using LoadBalancer IP.<br><b>Workaround:</b> CNE common services type can be set as ClusterIP manually. |

**Table 4-9 CNC Console 1.6.0 Customer Known Bugs**

| Bug Number | Severity | Found in Release | Title  | Customer Impact  |
|------------|----------|------------------|--|--|
| 31355530   | Minor    | 1.1.0            | CNCC IAM - Unable to remove assigned User Role                             | User will be able to add roles but user will not be able to remove the assigned roles.<br><b>Workaround:</b> Delete user and recreate user with required role.   |
| 32291223   | Minor    | 1.5.0            | CNCC : CNE Common Services type should be ClusterIP when accessed via CNCC | User will be able to access CNE common services directly using LoadBalancer IP.<br><b>Workaround:</b> CNE common services type can be set as ClusterIP manually. |

Table 4-10 CNC Policy 1.11.0 Customer Known Bugs

| Bug Number | Severity | Found in Release | Title   | Customer Impact  |
|------------|----------|------------------|---|--|
| 32650908   | 2        | 1.11.0           | Diam-GW does not connect to pcrf automatically  | Diam-GW does not connect to pcrf automatically<br><br><b>Workaround</b> - In Diameter Config Map set "responseOnly=true" for PCRF Core.  |
| 32650916   | 2        | 1.11.0           | Diamgw throws "No OCS/SH peer to send msg" even when it connected successfully                  | After diamgateway connects to OCS successfully, when it receives request to fetch for Sy, Sh datasource subscriber profile, diamgateway throws No OCS configured<br><br><b>Workaround</b> - Need to create Realm base Diamter Routing Table keeping both identity and name as hosts name |
| 32654621   | 3        | 1.11.0           | Sub-Policies which are called using "deprecated call Policy blocks" are not exported            | "call Policy" block when used in a policy is not able to export sub-policy.<br><br>This block is already deprecated and "call_policy_v2" is the new block to use.  |
| 32650967   | 3        | 1.11.0           | Export Report not generating if the policy table of the policy got deleted                      | There is no impact in export functionality. Export report will skip reporting the failure for the record that was deleted.   |
| 32650938   | 3        | 1.11.0           | Failed to process metrics with java.lang.NullPointerException on Sm-create when BSF_URL is used | No impact. Customers can use the real BSF URL. SM-service will throw exception when binding operation is enabled and local BSF configuration is used. This will lead to metric not getting pegged  |

**Table 4-10 (Cont.) CNC Policy 1.11.0 Customer Known Bugs**

| Bug Number | Severity | Found in Release | Title   | Customer Impact   |
|------------|----------|------------------|---|---|
| 32650943   | 3        | 1.11.0           | SM Egress Metric is not pegged for BSF interactions | Following two metrics will not be useful for SM to BSF intercatctions <ul style="list-style-type: none"> <li>ocpm_egress_request_total</li> <li>ocpm_egress_response_total</li> </ul> |

**Table 4-11 CNE 1.8.0 Customer Known Bugs**

| Bug Number | Severity | Found in Release           | Title   | Customer Impact   |
|------------|----------|----------------------------|---|---|
| OCCNE-3903 | 4        | 1.7.0                      | Kubespray task for applying cert issuer fails due to race condition which results in installation failure | Installation fails on k8s install stage. <b>Workaround:</b> Skip cert manager installation on next rerun and continue with common services and db tier installation on failure.                     |
| OCCNE-3743 | 3        | 1.4.0, 1.5.0, 1.6.0, 1.7.0 | Modify NETWORK_INTERFACE_FAILED alert to fire separate alert for gen10 and gen8 h/w                       | The current definition of NETWORK_INTERFACE_FAILED alert sends a false alarm for gen10 hardware. <b>Workaround:</b> Alerts can be modified on a per-site basis if this issue is of high importance. |
| OCCNE-3874 | 3        | 1.7.0                      | LB Controller cannot talk to TLS-enabled OpenStack  | No load balancing service available <b>Workaround:</b> Manually copy the OpenStack certificate to the LB Controller.  |

Table 4-11 (Cont.) CNE 1.8.0 Customer Known Bugs

| Bug Number | Severity | Found in Release | Title   | Customer Impact  |
|------------|----------|------------------|---|--|
| OCCNE-3453 | 4        | 1.7.0            | Geo-replication met with "Error_code: 1296; handler error HA_ERR_ROWS_EVENT_APPLY" error      | <p>We observed following behavior:</p> <ul style="list-style-type: none"> <li>Established replication between two sites 1 &amp; 2</li> <li>Records are getting replicated from Site 1 to Site 2</li> <li>Records are not getting replicated from Site 2 to Site 1</li> </ul> <p>This error is happening on both BM and vCNE installation.</p> <p><b>Workaround:</b> Set EventLogBufferSize to 64K. You can use mcm client to do this:</p> <pre>set EventLogBufferSize:n dbmtd=65536 occnendbcluster;</pre> |
| OCCNE-2534 | 3        | 1.4.0            | The openstack LDAP password should be hidden from the pipeline logs                           | NA   |
| OCCNE-1428 | 3        | 1.0.0, 1.2.0     | node_exporter generating error logs   | <p>Minor impact of an error be logged each minute from Prometheus Node Exporter.</p> <p><b>Workaround:</b> NA</p>  |
| OCCNE-3897 | 2        | 1.8.0            | CIS Based Linux Hardening - OL8   | NA   |
| OCCNE-1658 | 2        | 1.2.0            | Pods failover takes approximately 6 mins to start when kubernetes node is failed is restarted | <p>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.</p> <p><b>Workaround:</b> NA</p>   |

Table 4-11 (Cont.) CNE 1.8.0 Customer Known Bugs

| Bug Number | Severity | Found in Release | Title  | Customer Impact   |
|------------|----------|------------------|--|---|
| OCCNE-3523 | 2        | 1.7.0            | istio preventing teardown of clusters  | Iterating cluster creation/ destruction in our lab environment is made much more laborious, as the cluster destruction hangs in Jenkins, and it needs manual intervention to delete all resource though the OpenStack GUI.<br><br>If the manual destruction is not performed, we orphan resources in our OpenStack tenancy, and this leads to collisions use of our limited allocated resources.<br><br><b>Workaround:</b> NA |
| OCCNE-3485 | 3        | 1.4.0            | Updating the Alerts, Varbind and alert groups of prometheus.                       | NA  |
| OCCNE-2965 | 3        | 1.5.0            | Updating the labels and annotations in the dbtier services                         | NA  |
| OCCNE-3290 | 3        | 1.7.0            | Install for fixedip deployment failed  | NA  |
| OCCNE-2080 | 3        | 1.4.0            | k8s_install pipeline process fails due to time out trying to access yum.oracle.com | NA  |
| OCCNE-3378 | 4        | 1.7.0            | vCNE/Metallb - genLbCtrlData.py script fails using IP ranges                       | <b>Workaround:</b> Change the mb_configmap.yaml file IPs to a list or a cidr.   |
| OCCNE-3294 | 4        | 1.8.0            | Change in default namespace for PCF-ATS  | <b>Workaround:</b> Log in to Jenkins GUI : Configure: Advanced Project Option: Pipeline Script: -d ocats (not working)<br><br>Pipeline Script: -d ocpcf (modified to 'ocpcf'...in working case)<br><br>FIX: This should ideally be set to default value 'ocpcf' in 1.8.0.   |



Table 4-11 (Cont.) CNE 1.8.0 Customer Known Bugs

| Bug Number | Severity | Found in Release    | Title  | Customer Impact  |
|------------|----------|---------------------|--|--|
| OCCNE-991  | 2        | 1.0.0, 1.1.0, 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.<br><b>Workaround:</b> NA  |
| OCCNE-1398 | 4        | 1.0.0, 1.2.0        | Can't ssh to enclosure switches after configure from procedure                       | Minimal impact since there is a simple workaround.<br>The workaround is to ssh to OA then from OA "connect interconnect 1(1 for switch1 or 2 for switch2)" to access enclosure switches. It is an easy workaround. I will see how to fix the ssh access later. |
| OCCNE-3765 | 3        | 1.8.0               | Can't open occne-kibana GUI  | NA   |
| OCCNE-3524 | 3        | 1.7.0               | Sporadic k8s_install failure 'timeout (12s) waiting for privilege escalation prompt' | NA   |
| OCCNE-3311 | 3        | 1.7.0               | 1.7.0-rc.3 services restarting often. Test failures on services periodically         | NA   |
| OCCNE-3310 | 3        | 1.7.0               | BM Deploy CNE_SCAN fails on littlefinger (2 bastion) cluster                         | NA   |
| OCCNE-3312 | 3        | 1.7.0               | 1..70-rc.3 BM deploy kubespray failure   | NA   |
| OCCNE-1579 | 3        | 1.3.0               | Bastion host udp port domain unreachable traffic from tcpdump                        | NA   |
| OCCNE-3121 | 3        | 1.7.0               | Security Hardening: Docker hardening in provision should be fixed/enabled            | NA   |
| OCCNE-3122 | 3        | 1.7.0               | Security Hardening 'rpm_verify_permissions' should be fixed/enabled                  | NA   |
| OCCNE-2386 | 3        | 1.4.0               | Many network interface setting DEFROUTE=yes need to change to DEFROUTE=no            | NA   |
| OCCNE-2384 | 3        | 1.4.0               | The pxe_config_nic_list in hosts.ini for Gen10 blade server doesn't work well        | NA   |

Table 4-11 (Cont.) CNE 1.8.0 Customer Known Bugs

| Bug Number | Severity | Found in Release          | Title                                    | Customer Impact |
|------------|----------|---------------------------|--|-----------------|
| OCCNE-2505 | 3        | 1.4.0,<br>1.5.0,<br>1.6.0 | Worker nodes randomly becoming Not Ready | NA              |

Table 4-12 NRF 1.11.0 Customer Known Bugs

| Bug Number | Severity | Found in Release | Title  | Customer Impact   |
|------------|----------|------------------|--|---|
| 32623176   | 4        | 1.10.0           | RejectionReason to be added in NfAccessToken response metric                                       | Reason for rejection of the AccessToken Request can't be known by looking into the metric |
| 32623215   | 4        | 1.9.0            | Add NfUpdate Patch Operation with Unknown attribute are getting dropped silently and returning 200 | NF will not get notified that some of the attributes didn't get updated in NRF.           |

Table 4-13 SCP 1.11.0 Customer Known Bugs

| Bug Number | Severity | Found in Release | Title  | Customer Impact  |
|------------|----------|------------------|--|--|
| 30731782   | Minor    | 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.<br>For now customer impact is minimal to no.<br><b>Workaround:</b> None.<br><b>Note:</b> This limitation is not present in SCP 1.10 onwards. |

Table 4-13 (Cont.) SCP 1.11.0 Customer Known Bugs

| Bug Number | Severity | Found in Release | Title  | Customer Impact  |
|------------|----------|------------------|--|--|
| 30731844   | Minor    | 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.<br><b>Workaround:</b> None.  |
| 30731829   | Minor    | 1.4              | SCPC-Pilot is taking high CPU while applying updates if number of equivalent profiles/ ServiceInstances are exceeding 100  | There may be delay in rule creation if profiles are large in numbers which can cause some call failures.<br><b>Workaround:</b> None.<br><b>Note:</b> This limitation is not present in SCP 1.10 onwards. |

## UDR 1.11.0 Customer Known Bugs

| Bug Number | Severity | Found in Release | Title   | Customer Impact/WA  |
|------------|----------|------------------|---|---|
| 30774755   | 3        | 1.4.0            | Headers for few resources are not implemented as per spec 29505-v15.4.0     | No Impact   |
| 32631173   | 3        | 1.11.0           | udr_rest_request_total not pegged for Unsupported Media Type messages.      | No Impact   |
| 32631219   | 3        | 1.11.0           | PUT/POST request for policy-data/UDM with empty payloads returns 5xx errors | No Impact   |
| 32631240   | 3        | 1.11.0           | UDR returns 5012 when vsaLevel set to either dnn or nssai                   | No 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.                                 |

| Bug Number | Severity | Found in Release | Title   | Customer Impact/WA                                       |
|------------|----------|------------------|---|--|
| 31877256   | 4        | 1.8.0            | ProvGw: GET response sometimes does not have segment1 related data for subscriber does not exist case | No impact. It is intermittent issue.                     |
| 32377439   | 4        | 1.10.0           | De-Registration fails when egressgateway goes down before nrf-client during UDR deletion              | No impact  |
| 32377341   | 4        | 1.10.0           | Fetch UDM authentication subscription on UDR returns Internal Server Error                            | Occurs only with cnDBTier. Possible bug on MySQL Cluster |