Oracle® Communications

Cloud Native Core Release Notice

Release 2.3.0

F34860-06

July 2022

Oracle Communications Cloud Native Core Release Notice, Release 2.3.0

F34860-06

Contents

My Oracle Support

My Oracle Support (https://support.oracle.com) is your initial point of contact for all product support and training needs. A representative at Customer Access Support can assist you with My Oracle Support registration.

Call the Customer Access Support main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. When calling, make the selections in the sequence shown below on the Support telephone menu:

1. Select **2** for New Service Request.
2. Select **3** for Hardware, Networking and Solaris Operating System Support.
3. Select one of the following options:
    - For Technical issues such as creating a new Service Request (SR), select **1**.
    - For Non-technical issues such as registration or assistance with My Oracle Support, select **2**.

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

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

What's New In This Guide

This section introduces the documentation updates in Oracle Communications Cloud Native Core (CNC) network elements for Release 2.3.0.

New and Updated Sections for OSO Release 1.6.3

The following sections are updated for OSO Release 1.6.3:

- Resolved Bug List: Bugs resolved in OSO 1.6.3 are added.

New and Updated Sections for OSO Release 1.6.2

The following sections are updated for OSO Release 1.6.2:

- Resolved Bug List: Bugs resolved in OSO 1.6.2 are added.

New and Updated Sections for CNC Policy Release 1.8.4

The following sections are updated for CNC Policy Release 1.8.4:

- Resolved Bug List: Bugs resolved in CNC Policy 1.8.4 are added.

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 2.3.0.

Cloud Native Environment (CNE)

Cloud Native Environment (CNE) 1.6.0 provides the following major feature in this release:

- Operations Services Overlay Enhancements: OSO packaging has been modified to support the CSAR format. For more information, see *Operations Services Overlay Installation Guide*.
- DB Tier Overlay Enhancements: DB Tier Overlay packaging has been modified to support the CSAR format. For more information, see *Cloud Native Core DB Tier User Guide*.
- Virtual Infrastructure: Support has been added for a number of OpenStack infrastructure options, including:
  - Use TLS to access the OpenStack Controller
  - Use config_drive
  - Use external DNS
  - Use non-Nova availability zones

  For more information, see *Cloud Native Environment Installation Guide*.
- Bare Metal Infrastructure: Generic support has been added for deploying OC-CNE on new hardware types. For more information, see *Cloud Native Environment Installation Guide*.
- New vCNE Load Balancer: MetalLB has been added as a load balancer for virtualized deployments. For more information, see *Cloud Native Environment Installation Guide*.
- Automated Data Tier Maintenance Operations: Automated repair for several common failure scenarios has been included in this release. For more information, see *Cloud Native Environment Installation Guide*.
- CNE 1.6.0 updates Kubernetes to version 1.17.5.

Cloud Native Core Console (CNCC)

Cloud Native Core Console (CNCC) 1.3.0 has been updated with the following enhancements:

- CNCC Helm Test : The new Helm Test feature validates the successful CNCC installation along with readiness (Readiness probe url configured will be checked for success) of all the pods. The pods that needs to be checked, will be based on the namespace and label selector configured during the helm test configurations.
- Metric support has been introduced for CNCC Core and CNCC IAM Ingress Gateway. For more information on the metric details, see *Cloud Native Core Console User's Guide*.

- CNCC 1.3.0 is compatible with the latest version of the following Network Functions (NF):
  - SCP 1.8.0
  - NRF 1.8.0
  - UDR 1.8.0
  - CNC Policy 1.8.0
- The following GUI enhancements is introduced in CNCC 1.3.0:
  - New screen for UDR Diameter Service
  - NRF System options screen is updated as per latest API changes
  - Policy Import functionality has been improved for better user experience

Cloud Native Core Policy (CNC Policy)

CNC Policy 1.8.0 has been updated with the following enhancements:

- OCCNE and OSO Integration : CNC Policy and PCF supports OSO integration. For more information on integrating CNC Policy with OSO, see *Oracle Communications Cloud Native Core Policy Installation Guide*.
- Converged Diameter Gateway and Binding Service Enhancements : With this enhancement, new diameter metrics have been added. For more information on Binding Service and metrics, see *Oracle Communications Cloud Native Core Policy User's Guide*.
- Nudr to support OperatorSpecificData : CNC Policy supports custom JSON feature that enables flexible data schema for policy validation from Nudr interface. This enhancement allows you to configure flexible data schema as part of OperatorSpecificData and apply policies based on the data set. For more information, see *Oracle Communications Cloud Native Core Policy User's Guide* and *Oracle Communications Cloud Native Core Policy Design Guide*.
- Policy Action for bulk PCC Rule Removal: Starting with CNC Policy Release 1.8.0, policy complexity has been reduced by enabling bulk PCC Rule Removal for pre-defined and dynamic rules. For more information on Policy Action for bulk PCC Rule Removal, see *Oracle Communications Cloud Native Core Policy Design Guide.*
- Spending Limit Counter - With this enhancement, Policy solution enables you to use activation time in pending policy counter as input to the Condition Data for either activation time or deactivation time. This functionality is available for condition data used by PCC rules and session rules. For more information on spending limit pending counter, see *Oracle Communications Cloud Native Core Policy User's Guide* and *Oracle Communications Cloud Native Core Policy Design Guide*.
- Policy Event Records : Policy Event Records feature allows you to view transaction related information that includes input data set, policies that were evaluated and resulting policy actions from any transactions. For more information on configuration parameters related to policy event records, see *Oracle Communications Cloud Native Core Policy User's Guide.*
- Subscriber Activity Logging for UDR notification: You can now capture and monitor subscriber logs for UDR/CHF notifications and associated call flow in Session Management (SM) and egress gateway. For more information on subscriber

activity logging, see *Oracle Communications Cloud Native Core Policy User's Guide*.

- Dynamic override for Policy Data Configurations: With this feature, an operator can override and/or update attributes in real-time via policy actions. This feature is currently applicable to PCC Rules and Session Rules that were predefined at PCF. For more information on how to override policy data configurations dynamically, see Oracle Communications Cloud Native Core Policy Design Guide.
- Support for XFCC Header: With this enhancement, support for PCF as a producer has been added, to check, if SCP which has sent the HTTP request is the same proxy consumer or client, which is expected to send a HTTP2 request. This is achieved by comparing the FQDN of SCP present in the “x-forwarded-client-cert” (XFCC) of http2 header, with the FQDN of the SCPs configured in PCF. For more information on configurable parameters for XFCC header, see *Oracle Communications Cloud Native Core Policy Installation Guide*.
- Support for Session Retry and Alternate Route Service: In previous releases, CNC Policy and PCF were being configured with primary and secondary NRF statically and limiting to a specific number. Starting with CNC Policy Release 1.8.0, session retry enables the alternate recovery mechanisms to mitigate impact of any unavailable resource. Policy system provides flexible and configurable retry behavior for selected interfaces. To support this behavior, SRV Records has been added. This would add more options for NF FQDN to be configured and maintained dynamically at the DNS Server, which can be further selected by PCF, when there is an NF failure. For more information on configuring retry profile, see *Oracle Communications Cloud Native Core Policy User's Guide* and for more information on configurable parameters for alternate route service (DNS-SRV), see *Oracle Communications Cloud Native Core Policy Installation Guide*.

CNC NF Data Collector

Cloud Native Core Network Function Data Collector Tool 1.1.0 has below enhancements:

- Information on how to view and delete NF logs, metrics, and traces. For more information, see *Cloud Native Core Network Function Data Collector User's Guide*.
- Appendices to understand logs and metrics inclusion filter keywords. For more information, see *Cloud Native Core Network Function Data Collector User's Guide*.
- Information on how to remove pending resources from namespace. For more information, see *Cloud Native Core Network Function Data Collector User's Guide*.
- Support of K8 Namespace in Network Function Deployment data collection tool: This feature has been introduced since there can be multiple helm releases in same namespace. After new enhancements, helm specific data will also be collected belonging to entered namespace. For more information, see *Cloud Native Core Network Function Data Collector User's Guide*.
- Support of path for data collection output: Starting with CNC NF Data Collector Tool version 1.1.0, path for data collection output has been made configurable. For more information, see *Cloud Native Core Network Function Data Collector User's Guide*.

Cloud Native Diameter Routing Agent (CnDRA)

There are no new features or updates implemented in CNC 2.3.0 release.

Binding Support Function (BSF)

There are no new features or updates implemented in CNC 2.3.0 release.

Inter-Working Function (IWF)

There are no new features or updates implemented in CNC 2.3.0 release.

Network Exposure Function (NEF)

There are no new features or updates implemented in CNC 2.3.0 release.

Network Repository Function (NRF)

OCNRF 1.8.0 has been updated with the following enhancements:

- Per NF Heartbeat Configuration Enhancement: OCNRF supports Per NF Type configuration for heartbeat range and allowed heartbeat miss count. For more information, see *Oracle Communications Network Repository Function User's Guide*.
- NF Authentication using TLS Certificate: OCNRF authenticates consumer NF by Validating NF identity from TLS Certificate before allowing to use any NRF Services. For more information, see *Oracle Communications Network Repository Function User's Guide*.
- AccessToken Request Validation: OCNRF authorizes the consumer NF by applying local policy before issuing Access Token. For more information, see *Oracle Communications Network Repository Function User's Guide*.
- Dynamic Log Level change: OCNRF supports changing Log level dynamically for nfregistration, nfsubscription, nfdiscovery, nfaccesstoken, nrfconfiguration and nrfauditor micro-services. Remaining services, such as ocnrf-app-info, ingressgateway and egressgateway, continues to use helm based log level configuration. For more information, see *Oracle Communications Network Repository Function User's Guide*.
- Alerts and metrics: Supports additional System Level and Application level alerts and metrics. For more information, see *Oracle Communications Network Repository Function User's Guide*.

Network Slice Selection Function (NSSF)

There are no new features or updates implemented in CNC 2.3.0 release.

Service Communication Proxy (SCP)

SCP 1.8.0 has been updated with the following enhancement:

- Aspen Service Mesh 1.4.6-am9 (ASM) Integration with OSO: The Aspen Service Mesh integration supports inter-NF communication. The service mesh integration supports the services by deploying a special sidecar proxy in the environment to intercept all network communication between microservices. For more information, see *Service Communication Proxy Installation Guide.*

- Optional ClusterRole and ClusterRoleBinding for SCP deployment: This feature provides user with the option to choose between using or not using cluster role binding for SCP. For more information on configuring ClusterRoleBinding, see *Service Communication Proxy Installation Guide.*

Security Edge Proxy Protection (SEPP)

There are no new features or updates implemented in CNC 2.3.0 release.

Unified Data Management (UDM)

There are no new features or updates implemented in CNC 2.3.0 release.

Unified Data Repository (UDR)

UDR 1.8.0 has been updated with the following enhancements:

- Diameter configuration on CNC Console: UDR users can now configure Diameter Service using CNC Console. For more information, see *Cloud Native United Data Repository User's Guide*.
- OAuth2 support on UDR/SLF: UDR supports OAUTH2 authentication and tokens for ingress traffic. For more information on the relevant metrics, see *Cloud Native United Data Repository User's Guide*, and for information on creating certificate, see *Cloud Native United Data Repository Installation and Upgrade Guide*.
- Migration of 4G Policy Subscriber's data to 5G UDR: Using Migration Tool, UDR Users can migrate 4G UDR subscribers information to 5G UDR. For more information on migration tool, see *Cloud Native United Data Repository User's Guide.*.
- Bulk Import Provisioning: Using Bulk Import tool, UDR users can import subscriber’s data for PCF and SLF in bulk, in the .csv format. For more information on installing the Bulk Import tool, see *Cloud Native United Data Repository Installation and Upgrade Guide*, and for instructions on using the Bulk Import tool, see *Cloud Native United Data Repository User's Guide*.
- Provisioning Gateway Enhancements: Starting with Release 1.8.0, user can disable Provisioning when segment is not reachable. This procedure covers detecting failed SLF segment, removing that failed segment from network, fixing the issue, and then restoring the segment back to the network. It also covers information on Auditor service, its report types format, and method to generate auditor service reports. For more information on handling SLF Segments, see *Cloud Native United Data Provisioning Gateway Guide*.
- Supports default Alerts for UDR and Provisioning Gateway: For information on alerts related to UDR, see *Cloud Native United Data Repository User's Guide*, and for information on alerts for Ingress Traffic related to Prov GW, see *Cloud Native United Data Provisioning Gateway Guide*.
- Integrated with ASM: UDR and Provisioning Gateway users can enable service mesh by following instructions given as an appendix in the *Cloud Native United Data Repository Installation and Upgrade Guide* or *Cloud Native United Data Provisioning Gateway Guide*.

- Consolidated PCF provisioning API: For information on consolidated PCF provisioning API, see *Cloud Native UDR REST Specification Guide*.
- Quota support using Diameter Sh Interface: For information on quota support, see *Cloud Native United Data Repository User's Guide*.

3

Media and Documentation

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

Media Pack

This section lists the media package for Cloud Native Core 2.3.0. For downloading the package, refer to MOS.

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

Table 3-1 Media Pack Contents for Cloud Native Core 2.3.0

Description	Versions	ATS Test Cases Included	Upgrade	Compliance
Oracle Communications Cloud Native Core Automated Testing Suite (ATS)	1.3.0	Y	Fresh Installation	Compatible with CNE 1.5.0
Oracle Communications Cloud Native Core Binding Support Function (BSF)	1.5.1	N	Fresh Installation	Compatible with NRF 1.7.0 and UDR 1.7.0, and CNC Policy 1.8.0
Oracle Communications Cloud Native Core Binding Support Function (BSF)	1.5.0	N	Fresh Installation	Compatible with NRF 1.7.0 and UDR 1.7.0, and CNC Policy 1.7.1
Oracle Communications Cloud Native Core Console (CNCC)	1.3.0	NA	Fresh Installation	Compatible with SCP 1.8.0, NRF 1.8.0, UDR 1.8.0, CNC Policy 1.8.0, CNE 1.5.0, and CNE 1.6.0

Table 3-1 (Cont.) Media Pack Contents for Cloud Native Core 2.3.0

Description	Versions	ATS Test Cases Included	Upgrade	Compliance
Oracle Communications Cloud Native Core Cloud Native Environment (CNE)	1.6.0	NA	Supports fresh installation as well as upgrade from 1.5.0 to 1.6.0. For more information on installation or upgrading, see *Cloud Native Environment Upgrade Guide*.	NA
Oracle Communications Cloud Native Core Policy (CNC Policy)	1.8.4	Y	Supports only upgrade from 1.8.3 to 1.8.4. For more information on installation or upgrading, see *Oracle Communications Cloud Native Core Policy Installation and Upgrade Guide*.	Compatible with BSF 1.5.1, NRF 1.8.0, and UDR 1.8.0
Oracle Communications Cloud Native Core Policy (CNC Policy)	1.8.3	Y	Supports only upgrade from 1.8.2 to 1.8.3. For more information on installation or upgrading, see *Oracle Communications Cloud Native Core Policy Installation and Upgrade Guide*.	Compatible with BSF 1.5.1, NRF 1.8.0, and UDR 1.8.0
Oracle Communications Cloud Native Core Policy (CNC Policy)	1.8.2	Y	Supports only upgrade from 1.8.1 to 1.8.2. For more information on installation or upgrading, see *Oracle Communications Cloud Native Core Policy Installation and Upgrade Guide*.	Compatible with BSF 1.5.1, NRF 1.8.0, and UDR 1.8.0

Table 3-1 (Cont.) Media Pack Contents for Cloud Native Core 2.3.0

Description	Versions	ATS Test Cases Included	Upgrade	Compliance
Oracle Communications Cloud Native Core Policy (CNC Policy)	1.8.1	Y	Supports only upgrade from 1.8.0 to 1.8.1. For more information on installation or upgrading, see *Oracle Communications Cloud Native Core Policy Installation and Upgrade Guide*.	Compatible with BSF 1.5.1, NRF 1.8.0, and UDR 1.8.0
Oracle Communications Cloud Native Core Policy (CNC Policy)	1.8.0	Y **Note**: Not applicable to: • Converged Diameter Gateway Enhancement • Diameter Gateway Scaling • Nudr support for OperatorSpecificData • Policy Event Records • Diameter Gateway Metrics - Phase 1	Supports fresh installation as well as upgrade from 1.7.x to 1.8.0. For more information on installation or upgrading, see *Oracle Communications Cloud Native Core Policy Installation Guide*.	Compatible with BSF 1.5.0, NRF 1.8.0, and UDR 1.8.0
Oracle Communications Cloud Native Core Diameter Routing Agent (CnDRA)	1.6.0	NA	Fresh Installation	NA
Oracle Communications Cloud Native Core Inter-Working Function (IWF)	1.5.0	NA	Fresh Installation	Compatible with BSF 1.5.0, NRF 1.7.0, UDR 1.7.0, and compliant with 3GPP version 15.5
Oracle Communications Cloud Native Core Network Exposure Function (NEF)	1.2.0	NA	Fresh Installation	NA
Oracle Communications Cloud Native Core Network Repository Function (NRF)	1.8.0	Y **Note**: Not applicable to: • New Alerts • Dynamic Log Level change	Fresh Installation	Compatible with network functions which are compliant with 3GPP Release 29.510 v15.5 (September 2019)

Table 3-1 (Cont.) Media Pack Contents for Cloud Native Core 2.3.0

Description	Versions	ATS Test Cases Included	Upgrade	Compliance
Oracle Communications Cloud Native Core Network Slice Selection Function (NSSF)	1.4.0	NA	Fresh Installation	Compatible with any NRF, AMF that supports 3GPP Release 15.5 Specs
Oracle Communications Cloud Native Core Service Communication Proxy (SCP)	1.8.0	Y	Fresh Installation	Compatible with CNE 1.4.0, CNE 1.5.0 and CNE 1.6.0
Oracle Communications Cloud Native Core Security Edge Protection Policy (SEPP)	1.3.0	NA	Fresh Installation	NA
Oracle Communications Cloud Native Core Unified Data Repository (UDR)	1.8.0	Y **Note**: Applicable only to UDR-SLF	Fresh Installation	Compatible with CNE 1.5.0, CNE 1.6.0, NRF 1.7.0, and NRF 1.8.0
Oracle Communications Cloud Native Core Unified Data Management (UDM)	1.1.0	N	Fresh Installation	NA

Documentation Pack

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

4 Resolved and Known Bugs

This chapter lists the resolved and known bugs for Cloud Native Core release 2.3.0.

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

Severity Definitions

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

Severity 1

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

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

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

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

Severity 2

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

Severity 3

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

Severity 4

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

Resolved Bug List

The following resolved bugs tables list the bugs that are resolved in Cloud Native Release 2.3.0.

Table 4-1 OSO 1.6.3 Resolved Bugs

Bug Number	Severity	Found in Release	Title
33679493	3	1.6.2	OSO 1.6.2 pods missing podLabels and Image names have invalid prefixes
33650882	3	1.6.2	OSO 1.6.2 pods missing podLabels and Image names have invalid prefixes

Table 4-2 OSO 1.6.2 Resolved Bugs

Bug Number	Severity	Found in Release	Title
32224057	3	1.6.1	OSO: Targets oracle-cnc-service needs extra configurations
32224078	3	1.6.1	Remove TLS configurations from alertmanager
32224122	3	1.6.1	Adding support for PVC for Alertmanager
32224165	3	1.6.1	Disable Pushgateway Support
32224242	3	1.6.1	Increase Alertmanager Resource limits
32224256	3	1.6.1	Convert Descriptor Version to Software Version

Table 4-3 OSO 1.6.1 Resolved Bugs

Bug Number	Severity	Found in Release	Title
32222455	3	1.6.0	Truncate OSO prometheus component's fixed names
32222301	1	1.6.0	OSO Values File must be fixed
32223999	3	1.6.0	Modify Labels in Scrape Configuration
32224024	3	1.6.0	Modify Labels in Scrape Alert Configuration

Table 4-4   CNE 1.6.0 Resolved Bugs

Bug Number	Severity	Found in Release	Title
30756164	3	1.3.0	OCCNE 1.3 Bare Metal Installation Failure -- Replication IP not configured on Sql Nodes during DBTier installation
30756201	4	1.3.0	OCCNE 1.3 Bare Metal Installation Failure -- Pipeline.sh is not documented. Must be continually restart on error
30371715	4	1.2.0	OCCNE 1.2.0 Installation Guide does not provide guidance on Firmware Version.

Table 4-5   CNC Console 1.3.0 Resolved Bugs

Bug Number	Severity	Found in Release	Title
31836979	Major	1.2.0	CNCC 1.2: SLF Data Provisioning
31825563	Medium	1.1.0	VzW ME Lab – CNCC 1.1 issues
31773454	Minor	1.2.1	In the custom values, the image names and tags are not set correctly.
31773492	Minor	1.2.1	CNCC 1.2.1-rc.1: CNCC-IAM pod template restricts the name length to 20 characters.
31855444	Minor	1.0.0	After installing CNCC-IAM, a user cannot login with the initial user name.
31855476	Minor	1.2.1-rc.1	CNCC 1.2.1-rc.1: Question on FQDN Support
31889461	Minor	1.2.1	SCP Canary Release edit does not function as expected
31890147	Minor	1.2.1	CNCC IAM DB SQL file causes replication failure

Table 4-6   BSF 1.5.1 Resolved Bugs

Bug Number	Severity	Found in Release	Title
31972868	3	1.5.0	Binding query is not successful in BSF Management when we have shotrthand IPv6 prefix used in both SM create and AAR-I.

Table 4-7   CNC Policy 1.8.4 Resolved Bugs

Bug Number	Severity	Found in Release	Title
32186027	2	1.8.1	PCF does not send SuppFeatures IE for PRA in SM Policy Association Response
32186184	3	1.8.3	Upgrade --> Rollback --> re-upgrade issue/failure

Table 4-8 CNC Policy 1.8.3 Resolved Bugs

Bug Number	Severity	Found in Release	Title
32140574	3	1.8.0	Rx message are missing when do subscriber trace
32140590	3	1.8.0	Egress logs are not captured in Subscriber Tracing
32140598	3	1.8.0	All PCF resources (e.g. hook job templates) not configured to receive customExtension allResources labels and annotations using global.customExtension.allResources for ASM integration
32140631	3	1.8.0	Support for Configurable Http2 Client Connections implementation
32140689	3	1.8.0	When call-rate of delete PDU session is bigger than 50, sm-service throws exception of Failed to call BSF

Table 4-9 CNC Policy 1.8.2 Resolved Bugs

Bug Number	Severity	Found in Release	Title
32179811	2	1.8.1	User Service Threads are growing unbounded

Table 4-10 CNC Policy 1.8.1 Resolved Bugs

Bug Number	Severity	Found in Release	Title
31959719	2	1.7.4	PCF sending Abort to AF during traffic call flow
31959847	2	1.7.4	PRE not processing policies because of permission issues of the directory
31960033	2	1.8.0	AAR-U not respond in PCF mode
31880917	3	1.8.0	On AAR Update, diam-gateway fails to fetch dependent SessionBindingMapping from binding service
31883568	3	1.7.3	Timestamp is not consistent across services and the format is not supported by Kibana
31895101	3	1.7.1	UDR user sm policy profile update notify message to ingress not logged
31959765	3	1.7.4	Support for Configurable Http2 Client Connections implementation

Table 4-11 CNC Policy 1.8.0 Resolved Bugs

Bug Number	Severity	Found in Release	Title
31883568	3	1.7.3	REMOVE_ALL Policy Block is not working in PCF
31847912	2	1.7.1	Scaling is not working for nrf-discovery due to wrong deployment reference in HPA
31629612	3	1.7.1	One user-service pod throws error as "IllegalArgumentException" while other pod coming up properly

Table 4-12 NRF 1.8.0 Resolved Bugs

Bug Number	Severity	Found in Release	Title
31759596	4	1.7.0	DB-RTT and Response Processing Time metrics validation fails randomly
31866286	2	1.7.2	jobNames are exceeding the 63 character limit
31866323	3	1.7.0	nnrf-disc fails when TAI Query parameter is used
31866379	4	1.7.0	Grafana dashboard template includes time period set to 2020-07-06
31866498	4	1.5.0	Error in AMF to NRF registration because of *defaultNotificationSubscriptions*
31866529	4	1.5.0	Error in AMF registering to NRF because of *nfInstanceId* included in URL and body in different format (upper and lower case)
31866632	4	1.7.2	Timestamp keyword in log is resulting in log not coming in Kibana

Table 4-13 SCP 1.8.0 Resolved Bugs

Bug Number	Severity	Found in Release	Title
31868324	3	1.7.3	Add automatic quotes around annotations values using helm quote function
31868333	3	1.7.2	SS: Notification throws duplicate IpEndpoint validation error when within a profile two same services have only port present in *ipEndpoint*. The port present is same.
31877610	2	1.7.1	oscpw-router Envoy Filter port is not synced with gateway signaling port
31881944	4	1.7.1	Instead of having multiples summaries in ATS, have just one summary

Table 4-14 UDR 1.8.0 Resolved Bugs

Bug Number	Severity	Found in Release	Title
31608081	3	1.7.0	*UsageMonitoring* data request issue for UDR v15.3 PCF
31593712	3	1.7.0	Diameter request, where mandatory avps are missing, must be rejected
31618168	3	1.7.0	Diameter traffic fails when Data-Reference AVP is set to 0

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 4-15 BSF 1.5.1 Customer Known Bugs

Bug Number	Severity	Found in Release	Title	Customer Impact
31973019	3	1.5.0	S-NSSAI shall be Optional parameter in bsf discovery	User needs to pass the s-nssai as part of query parameters.

Table 4-16 CNC Console 1.3.0 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. Workaround: Delete user and recreate user with required role.

Table 4-17   CNC Policy 1.8.1 Customer Known Bugs

Bug Number	Severity	Found in Release	Title	Customer Impact
31972768	3	1.8.0	Config Client Connection to Config Server hangs when DB issues are encountered	This issue is observed when there are issues in database and config server not able to communicate with the database. When this happens service will not be able to get the new configuration from the database. Right now, this issue is observed in one particular cloud lab. **Workaround**: Database issue needs to be resolved and the affected service needs to be restarted.

Table 4-18   CNC Policy 1.8.0 Customer Known Bugs

Bug Number	Severity	Found in Release	Title	Customer Impact
31880875	2	1.8.0	Converged (PCF Mode): Sm service connection with PRE is breaking intermittently & sm-service throws up "Failed to call policy service" logs	This issue is intermittent and occurred in a call rate of 1250 TPS, and was seen eight times in a 12 hour run. When this issue occurs, the default policy will be applied.
31880883	3	1.7.1	timestamp is not consistent across services and the format is not supported by Kibana	User will not be able to sort and sequence the messages in Kibana board.
31880914	3	1.8.0	SM-Rx: Rx session mapping with IMSI/MSISDN fails with error 5065, though corresponding SM binding is available	During SM RX call flow, Rx with only IMSI/MSISDN identifiers without fails to fetch binding service information and respond back with error response 5065.
31886960	3	1.8.0	Bug 31886960 - SM-Binding: Metric for Binding delete does not increment on SM session deletion	Metrics for Binding delete is not incremented on successful SM session delete request.

Table 4-18 (Cont.) CNC Policy 1.8.0 Customer Known Bugs

Bug Number	Severity	Found in Release	Title	Customer Impact
31895171	3	1.8.0	SM & User-service are not able to connect to alternate service with default 8000 port(unified port)	SM & User will not be able to connect to alternate route service for in-session messages (Update/Delete/Update-Notify) and those transactions will fail.
31898693	3	1.8.0	On loss of connectivity with OCS, Diam Gateway failed to reconnect to OCS	Diam Gateway will not try to reconnect again after connectivity is lost between diam gateway to OCS server. **Workaround**: Restart the diam gateway pod.
31898707	3	1.8.0	Error Response(5065) for Gx request on switching OCS admin state from ON to OFF	On turning admin state of data source configuration from ON to OFF in CM GUI, Diam gateway will send error respond to Gx Call (5065).

Table 4-19 NRF 1.8.0 Customer Known Bugs

Bug Number	Severity	Found in Release	Title	Customer Impact
31866770	4	1.7.2	NRF service containers should not send HTTPS request to Sidecar container	Notification URI received with HTTPS scheme may fail with Service Mesh.
31866838	4	1.7.2	Propagating Jaeger Headers for Forwarding/SLF requests	Forwarding and SLF queries will not come under one parent Trace.
31866858	4	1.7.0	*replicationstatus* alert should not be raised when Geo-Redundancy feature is disabled.	Replication Down alert will be seen in a non-Geo-Redundant Deployment.

Table 4-20 SCP 1.8.0 Customer Known Bugs

Bug Number	Severity	Found in Release	Title	Customer Impact
30731782	3	1.2.0	Limit of VS size is limited to 1 Mb by etcd/k8s.	Impacts only if there are 100s of NFs with many service instances/NF and hence minimal impact for customer/ user. **Workaround**: None. This is limited by underlying platform.
30731844	3	1.3.0	Processing time of NRF notifications increases if more profiles (>10) with more many service instances (more than 10/profile)are registered. increase observed is 2-3 seconds more than previous registered in case of new registration. Updates also increases with more number of registered profiles.	There may be delay in rule creation if profiles are large in numbers. **Workaround**: None.
30731829	3	1.4.0	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 that can cause some call failures.

Table 4-21 UDR 1.8.0 Customer Known Bugs

Bug Number	Severity	Found in Release	Title	Customer Impact
30774742	4	1.3.0	UDR is not validating the conditional attributes for UDM APIs.	No impact. UDM (consumer of UDM APIs) does not send conditional attributes to UDR
30774750	4	1.3.0	Notify Service delays notifications to PCF during traffic run.	Notifications rate is limited in initial release.
30774755	3	1.4.0	Headers for few resources are not implemented as per spec 29505-v15.4.0.	No impact.
31877256	4	1.8.0	ProvGw: GET response sometimes does not have segment1 related data for subscriber does not exist case.	No impact. This issue is observed intermittently.
31889017	4	1.8.0	Issues observed on ProvGw on ASM machine	No impact. This issue is observed intermittently.