Oracle® Communications

Cloud Native Configuration Console Network Impact Report

Release 24.3.0
G10452-01
October 2024

Oracle Communications Cloud Native Configuration Console Network Impact Report, Release 24.3.0

G10452-01

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:

- 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.

Acronyms

The following table lists the acronyms and the terminologies used in the document:

Table Acronyms

Acronym	Description
A-CNCC Core	Agent CNC Console is a CNCC Core instance which manages local NF(s) and local OCCNE common services(s). A-CNCC is managed by M-CNCC. A-CNCC contains A-CNCC Core Ingress Gateway. A-CNCC has no IAM component. A-CNCC is also known as A-CNCC Core or aCncc Core.
AD	Active Directory
ASM	Aspen Service Mesh
BSF	Oracle Communications Cloud Native Core, Binding Support Function
CAPIF	Common API Framework
cnDBTier	Oracle Communications Cloud Native Core, cnDBTier
CNC Console	Oracle Communications Cloud Native Configuration Console
CNE	Oracle Communications Cloud Native Core, Cloud Native Environment
CNI	Container Network Interface
CNLB	Cloud Native Load Balancer
CS	Common Service
CRUD Operations	CREATE, READ, UPDATE, DELETE
ECDSA	Elliptic Curve Digital Signature Algorithm
EIR	Equipment Identity Register
HTTPS	Hypertext Transfer Protocol Secure
GRR	Geo Replication Recovery
IAM	Identity Access Management
Instance	NF or CNE common service managed by either M-CNCC Core or A-CNCC Core.
KPI	Key Performance Indicator
LDAP	Lightweight Directory Access Protocol
LDAPS	Lightweight Directory Access Protocol (Over SSL)
M-CNCC	Manager CNC Console or mCncc is a CNC Console instance which manages multiple A-CNCC and local instances. **Non OCI**: M-CNCC has two components M-CNCC IAM and M-CNCC Core **OCI**: M-CNCC has only M-CNCC Core component. M-CNCC IAM is substituted with OCI IAM.
M-CNCC IAM	Manager CNC Console IAM or M-CNCC IAM (also known as mCncc Iam) is an IAM component of M-CNCC. M-CNCC IAM contains M-CNCC IAM Ingress Gateway and M-CNCC IAM back-end microservices.

Table (Cont.) Acronyms

Acronym	Description
M-CNCC Core	Manager CNC Console Core or M-CNCC Core (also known as mCncc Core) is a core component of M-CNCC that provides GUI and API access portal for accessing NF and OCCNE common services. M-CNCC Core contains M-CNCC Core Ingress Gateway and M-CNCC Core back-end microservices.
M-CNCC Kubernetes cluster	Kubernetes cluster hosting M-CNCC
MC	Multi Cluster. In multi cluster, a single CNCC can manage NF instances that accessess different Kubernetes clusters.
MO	Mananged Objects
MOS	My Oracle Support
mTLS	Mutual Transport Layer Security
NEF	Oracle Communications Cloud Native Core, Network Exposure Function
NRF	Oracle Communications Cloud Native Core, Network Repository Function
OCI	Oracle Cloud Infrastructure
OCNADD	Oracle Communications Network Analytics Data Director
OCNWDAF	Oracle Communications Networks Data Analytics Function
OCNF	Oracle Communications Network Function
OSDC	Oracle Software Delivery Cloud
OSO	Oracle Communications Operations Services Overlay
PROVGW	Provisioning Gateway
REST API	Representational State Transfer Application Programming Interface
RBAC	Role Based Access Control
SAML	Security Assertion Markup Language
SBA	Service Based Architecture
SBI	Service Based Interface
SCP	Oracle Communications Cloud Native Core, Service Communication Proxy
SEPP	Oracle Communications Cloud Native Core, Security Edge Protection Proxy
Site	Kubernetes Cluster
SSO	Single Sign On
TLS	Transport Layer Security
UDR	Oracle Communications Cloud Native Core, Unified Data Repository
UE	User Equipment
URI	Subscriber Location Function

What's New in this Guide

This section introduces the documentation updates for release 24.3.x.

Release 24.3.0 - G10452-01, October 2024

Updated the following sections:

- Compatibility Matrix
- Common Services Load Lineup
- Software Requirements
- Orchestration
- CNC Console Features
- Supported Upgrade and Rollback Paths
- Helm

1 Introduction

The purpose of this document is to highlight the changes made in CNC Console from release 24.2.x to release 24.3.0. These changes may have an impact on the customer network operations and must be considered by the customer while planning the deployment.

1.1 Compatibility Matrix

This section lists the versions of added or updated components in release 24.3.x. To know the list of all the supported versions, see *Oracle Communications Cloud Native Core Release Notes*.

> **Note**
>
> CNC Console supports N-2 NF versions during upgrade window. For example, CNC Console 24.3.x supports SCP 24.3.0, 24.2.x, and 24.1.x.
>
> If NFs are on older release (upto N-2), new features which have NF dependencies in the current release may not be available.

Release 24.3.0

The following table lists the versions of added or updated network functions in this release:

Table 1-1 CNC NF Compatibility Matrix

Network Functions	Compatible Versions
BSF	24.3.x
CAPIF	24.3.x
NEF	24.3.x
NRF	24.3.x
NSSF	24.3.x
Policy	24.3.x
SCP	24.3.x
SEPP	24.3.x
UDR	24.3.x

CNC Console is compatible with the following components:

Table 1-2 Compatibility Matrix

Component	Compatible Versions
ASM	1.14.6, 1.11.8, 1.9.8
CNE	24.3.x, 24.2.x, 24.1.x

Table 1-2 (Cont.) Compatibility Matrix

Component	Compatible Versions
cnDBTier	24.3.x, 24.2.x, 24.1.x
OCCM	24.3.x
OCI Adaptor	24.3.x
OCNADD	24.3.x
OCNWDAF	24.3.x
OSO	24.3.x, 24.2.x, 24.1.x
PROVGW	24.3.x

1.2 Common Services Load Lineup

This section lists the versions of added or updated common services in release 24.3.x. To know the list of all the supported versions, see *Oracle Communications Cloud Native Core Release Notes.*

Release 24.3.0

The following table lists the versions of added or updated common services in this release:

Table 1-3 Common Services Load Lineup

Common Service	Version
Debug-tool	24.3.1
Helm Test	24.3.2
Ingress Gateway	24.3.3

1.3 Software Requirements

This section lists the added or updated software required to install CNC Console release 24.3.x. For more information about software requirements, see *Oracle Communications Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide.*

Release 24.3.0

The following table lists the versions of added or updated software required to install this release:

Table 1-4 Software Requirements

Software	Version
HELM	3.14.2
Kubernetes	1.30.x, 1.29.x, 1.28.x
Podman	4.4.1
Prometheus	2.51.1

The following table lists the versions of additional software:

Table 1-5 Additional Software

Software	Version	Required For
FluentBit	1.9.4	Logging
Grafana	9.5.3	KPIs
Jaeger	1.60.0	Tracing
Kyverno	1.12.5	Logging
MetalLB	0.14.4	External IP
Opensearch	2.11.0	Logging
OpenSearch Dashboard	2.11.0	Logging
Prometheus	2.51.1	Metrics
snmp-notifier	1.2.1	Alerts

1.4 Orchestration

This section provides information about orchestration changes in release 24.3.x.

Release 24.3.0

The following table provides information about orchestration changes in this release.

Table 1-6 Orchestration

Orchestration Changes	Status	Notes
Support for in-service upgrade	Yes	The Console microservices are single pod. For information about upgrade and rollback, see Upgrading CNC Console and Rolling Back CNC Console sections in *Oracle Communications Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide.*
Changes in the custom_values.yaml file	Yes	For information about changes in the `custom_values.yaml` file, see Helm section.
Changes in the resource information for custom_values.yaml file	No	• No changes in CNC Console resource information. • cnDBTier resource profile is updated under `occncc_dbtier_custom_values.yaml` as per Console need.
Changes in the CSAR package	Yes	• CSAR package is updated as per latest release. **Note:** For more information on specific CSAR changes, contact My Oracle Support
Changes in Role-Based Access Control (RBAC) policy	No	No changes in Role-Based Access Control. For more information, see *Oracle Communications Cloud Native Configuration Console User Guide.*
Changes in Life Cycle Management (LCM) Operations	Yes	OCCM integration support is added which will be used for managing lifecycle of Console Certificates.

Table 1-6 (Cont.) Orchestration

Orchestration Changes	Status	Notes
Helm Test Support	Yes	Helm Test is supported. For more information, see "Performing Helm Test" section in *Oracle Communications Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide.*

1.5 Resource Requirements

This section lists the added or updated resource requirements in release 24.3.x. For more information about resource requirements, see *Oracle Communications Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide*.

Release 24.3.0

There is no change in the resource requirements in this release.

2 CNC Console Features

This chapter lists the added or updated features in release 24.3.x. For more information about the features, see *Oracle Communications Cloud Native Configuration Console User Guide.*

Release 24.3.0

CNC Console includes the following features or enhancements:

- **Support for TLS with Automated Certificate Management:** CNC Console supports automation of certificate lifecycle management in integration with Oracle Communications Cloud Native Core Certificate Manager (OCCM). This allows you to automatically create, renew, and delete certificates for a given CA, with the possibility to track previously created certificates and renew or delete them when required. For more information about OCCM, see the "Support for Automated Certificate Lifecycle Management" section in *Oracle Communications Cloud Native Configuration Console User Guide, Oracle Communications Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide*, and *Oracle Communications Cloud Native Core, Certificate Management User Guide.*
- **Support for Traffic Segregation:** CNC Console supports network segregation using Cloud Native Load Balancer (CNLB) to effectively manage ingress and egress traffic flows. CNE provides Cloud Native Load Balancer (CNLB) for managing networks used for ingress and egress traffic, as an alternate to the existing LBVM, lb-controller, and egress-controller solution. When this feature is enabled, CNE automatically uses CNLB to control ingress traffic. For managing the egress traffic, you must preconfigure the egress network details in the `cnlb.ini` file before installing CNE. This feature implements a least connection algorithm for IP Virtual Server (IPVS) based ingress distribution. For more information about this feature, see *Oracle Communications Cloud Native Configuration Console User Guide* and *Oracle Communications Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide.*
- **Support for Dual Stack (IPv6 preferred) on Dual Stack IPv4 preferred Infrastructure:** CNC Console can be deployed with IPV4 or IPV6 or both simultaneously. For more information about this feature, see *Oracle Communications Cloud Native Configuration Console User Guide* and *Oracle Communications Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide.*

3

Supported Upgrade and Rollback Paths

This chapter lists the supported upgrade and rollback paths in release 24.3.x. For more information about upgrade and rollback, see *Oracle Communications Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide.*

CNC Console Deployment Support Matrix

The following table provides details about the support of Console deployment features models for various network functions:

Table 3-1 CNC Console Deployment Model Matrix

Deployment Models	Policy	BSF	SCP	UDR	NRF	NEF	CAPIF	SEPP	NSSF	DD	PROVGW	NWDAF	OCCM
Model 1 - Single Cluster, Single Instance (Dedicated Console for each NF in a cluster)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Model 2 - Single Cluster, Multiple Instances (One Console for many NFs/ Instances in a cluster)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Table 3-1 (Cont.) CNC Console Deployment Model Matrix

Deployment Models	Policy	BSF	SCP	UDR	NRF	NEF	CAPIF	SEPP	NSSF	DD	PROVGW	NWDAF	OCCM
Model 3 - Multiple Clusters, Single Instance (Multiple clusters with single NF/ Instance in each cluster, M-CNCC/A-CNCC sitting in same/ different clusters)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Model 4 - Multiple Clusters, Multiple Instances (Multiple clusters with multiple NF/ Instance in each cluster, M-CNCC/A-CNCC sitting in same/ different clusters)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Release 24.3.0

Supported Upgrade Paths

The following table lists the supported upgrade paths in this release:

Table 3-2 Supported Upgrade Paths

Source Release	Target Release
24.2.x	24.3.x
24.1.x	24.3.x

Upgrade Impact:

There is no upgrade impact in this release.

Supported Rollback Paths

The following table lists the supported rollback paths in this release:

Table 3-3 Supported Rollback Paths

Source Release	Target Release
24.3.x	24.2.x
24.3.x	24.1.x

Rollback Impact

There is no rollback impact in this release.

4
Configuration

This chapter lists the configuration changes in release 24.3.x.

4.1 Helm

This section lists the Helm parameter changes in release 24.3.x. For more information about the Helm parameters, see *Oracle Communications Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide.*

Release 24.3.0

The following are the Helm parameters changes in this release:

1. **Dual Stack Support Feature:**
   a. In the custom values file, an option is provided to set the possible values for `cnccDeploymentMode` at the global level. An option is also provided at each microservice level to overwrite this value.

```
global:

  # Dual Stack Support
  # Possible values : IPv4, IPv6, IPv4_IPv6,IPv6_IPv4,ClusterPreferred
  cnccDeploymentMode: &cnccDeploymentMode ClusterPreferred


cncc-iam:
  kc:
    global:
      # Possible values : IPv4, IPv6,
IPv4_IPv6,IPv6_IPv4,ClusterPreferred
      deploymentMode: *cnccDeploymentMode

  ingress-gateway:
    global:
      # Possible values : IPv4, IPv6,
IPv4_IPv6,IPv6_IPv4,ClusterPreferred
      deploymentMode: *cnccDeploymentMode

    service:
      # Labels and Annotations that are specific to service
ingressgateway are added here.
      customExtension:
        labels: {}
        annotations: {}
        # This annotation metallb.universe.tf/loadBalancerIPs: IP1,IP2
is required to assign static IPs for service with
        # comma separated values, applicable for Dual stack support
RequireDualStack IP Family policy
        # metallb.universe.tf/loadBalancerIPs: ""
```

```
mcncc-core:
  cmservice:
    global:
      # Possible values : IPv4, IPv6,
IPv4_IPv6,IPv6_IPv4,ClusterPreferred
      deploymentMode: *cnccDeploymentMode

  ingress-gateway:
    global:
      # Possible values : IPv4, IPv6,
IPv4_IPv6,IPv6_IPv4,ClusterPreferred
      deploymentMode: *cnccDeploymentMode

    service:
      # Labels and Annotations that are specific to service
ingressgateway are added here.
      customExtension:
        labels: {}
        annotations: {}
        # This annotation metallb.universe.tf/loadBalancerIPs: IP1,IP2
is required to assign static IPs for service with
        # comma separated values, applicable for Dual stack support
RequireDualStack IP Family policy
        # metallb.universe.tf/loadBalancerIPs: ""

acncc-core:
  ingress-gateway:
    global:
      # Possible values : IPv4, IPv6,
IPv4_IPv6,IPv6_IPv4,ClusterPreferred
      deploymentMode: *cnccDeploymentMode

    service:
      # Labels and Annotations that are specific to service
ingressgateway are added here.
      customExtension:
        labels: {}
        annotations: {}
        # This annotation metallb.universe.tf/loadBalancerIPs: IP1,IP2
is required to assign static IPs for service with
        # comma separated values, applicable for Dual stack support
RequireDualStack IP Family policy
        # metallb.universe.tf/loadBalancerIPs: ""
```

b. The following field has been removed from the custom values file because the `deploymentMode` attribute updates the stack preference:

```
cncc-iam:
  kc:
    preferIpv6Stack:
      enabled: false
```

2. **Traffic Segregation:**

In the custom values file, an option is provided to add an annotation to set CNLB IP and network attachment:

```
cncc-iam:

  kc:
    keycloak:
      # Pod Annotation for cncc-iam-kc
      podAnnotations: {}
        #k8s.v1.cni.cncf.io/networks: ""

  ingress-gateway:
    # Labels and Annotations that are specific to deployment
ingressgateway are added here.
    deployment:
      customExtension:
        labels: {}
        annotations: {}
          #k8s.v1.cni.cncf.io/networks: ""
          #oracle.com.cnc/cnlb: '[{"backendPortName": "cncc-iam-port",
"cnlbIp": "","cnlbPort": ""}]'

    ports:
      # ContainerPort represents a network port in a single container
      containerPort: 8081
      containerPortName: cncc-iam-port
      containersslPort: 8443
      containersslPortName: cncc-iam-port
      actuatorPort: 9090


mcncc-core:
  ingress-gateway:
    # Labels and Annotations that are specific to deployment
ingressgateway are added here.
    deployment:
      customExtension:
        labels: {}
        annotations: {}
          #k8s.v1.cni.cncf.io/networks: ""
          #oracle.com.cnc/cnlb: '[{"backendPortName": "mcncc-core-port",
"cnlbIp": "","cnlbPort": ""}]'

    ports:
      # ContainerPort represents a network port in a single container
      containerPort: 8081
      containerPortName: mcncc-core-port
      containersslPort: 8443
      containersslPortName: mcncc-core-port
      actuatorPort: 9090


acncc-core:
  ingress-gateway:
    # Labels and Annotations that are specific to deployment
ingressgateway are added here.
```

```
    deployment:
      customExtension:
        labels: {}
        annotations: {}
          #k8s.v1.cni.cncf.io/networks: ""
          #oracle.com.cnc/cnlb: '[{"backendPortName": "acncc-core-port",
"cnlbIp": "","cnlbPort": ""}]'

    ports:
      # ContainerPort represents a network port in a single container
      containerPort: 8081
      containerPortName: acncc-core-port
      containersslPort: 8443
      containersslPortName: acncc-core-port
      actuatorPort: 9090
```

3. **TLSv1.3 Support in CNC Components**: In the custom values file, options have been provided to set the TLS version, `clientDisabledExtension`, `serverDisabledExtension`, `tlsNamedGroups`, and `clientSignatureSchemes` in the global level. Also an option is provided at each microservice level to overwrite these values.

```
############################################################
#            Section Start: global attributes              #
############################################################

global:
  tlsVersion: &tlsVersion TLSv1.2,TLSv1.3
  cipherSuites: &cipherSuites
    - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
    - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
    - TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
    - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
    - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
    - TLS_AES_256_GCM_SHA384
    - TLS_AES_128_GCM_SHA256
    - TLS_CHACHA20_POLY1305_SHA256

  #comma-separated-values To disable extension being sent in ClientHello
  #Remove ec_point_formats from clientDisabledExtension and
serverDisabledExtension in case golang version is lower than latest of 1.18
  clientDisabledExtension: &clientDisabledExtension
session_ticket,status_request,status_request_v2,psk_key_exchange_modes,pre_
shared_key,early_data,certificate_authorities,ec_point_formats
  #comma-separated-values To disable extension being sent from server
originated messages
  serverDisabledExtension: &serverDisabledExtension
session_ticket,status_request,status_request_v2,psk_key_exchange_modes,pre_
shared_key,early_data,ec_point_formats
  #comma-separated-values to allow the supported_groups extension values
  tlsNamedGroups:  &tlsNamedGroups
secp521r1,secp384r1,secp256r1,x448,x25519
  #comma-separated-values to allow the signature_algorithms extension
values
  clientSignatureSchemes: &clientSignatureSchemes
ecdsa_secp521r1_sha512,ecdsa_secp384r1_sha384,ecdsa_secp256r1_sha256,ed448,
```

```
ed25519,rsa_pss_rsae_sha512,rsa_pss_rsae_sha384,rsa_pss_rsae_sha256,rsa_pss
_pss_sha512,rsa_pss_pss_sha384,rsa_pss_pss_sha256,rsa_pkcs1_sha512,rsa_pkcs
1_sha384,rsa_pkcs1_sha256

##################################################################
#            Section Start  : cncc iam attributes            #
##################################################################
cncc-iam:
  kc:
    ldaps:
      service:
        ssl:
          tlsVersion: *tlsVersion
          cipherSuites: *cipherSuites

          clientDisabledExtension: *clientDisabledExtension
          tlsNamedGroups: *tlsNamedGroups
          clientSignatureSchemes: *clientSignatureSchemes

  ingress-gateway:
    clientDisabledExtension: *clientDisabledExtension
    serverDisabledExtension: *serverDisabledExtension
    tlsNamedGroups: *tlsNamedGroups
    clientSignatureSchemes: *clientSignatureSchemes

    service:
      ssl:
        tlsVersion: *tlsVersion

    cipherSuites: *cipherSuites

#########################################################################
#            Section Start  : manager cncc core attributes            #
#########################################################################
mcncc-core:
  ingress-gateway:
    clientDisabledExtension: *clientDisabledExtension
    serverDisabledExtension: *serverDisabledExtension
    tlsNamedGroups: *tlsNamedGroups
    clientSignatureSchemes: *clientSignatureSchemes

    service:
      ssl:
        tlsVersion: *tlsVersion

    cipherSuites: *cipherSuites

#########################################################################
#            Section Start  : agent cncc core attributes            #
#########################################################################
acncc-core:
  ingress-gateway:
    clientDisabledExtension: *clientDisabledExtension
    serverDisabledExtension: *serverDisabledExtension
    tlsNamedGroups: *tlsNamedGroups
    clientSignatureSchemes: *clientSignatureSchemes
```

```
service:
  ssl:
    tlsVersion: *tlsVersion

cipherSuites: *cipherSuites
```

4. **Changes to CNC Console cnDBTier custom values**:
   a. The following configurations are removed from the cnDBTier custom values file:

```
global:
    additionalndbconfigurations:
        mysqld:
            binlog_transaction_dependency_tracking: "COMMIT_ORDER"
        ndb:
            delayPerDataPod: 60
```

   b. The following configurations are added to the cnDBTier custom values file:

```
global:
  additionalndbconfigurations:
    replmysqld:
      relay_log_space_limit: 0
      max_relay_log_size: 0
    tcpemptyapi:
      SendBufferMemory: '2M'
      ReceiveBufferMemory: '2M'
      TCP_SND_BUF_SIZE: '0'
      TCP_RCV_BUF_SIZE: '0'

  ndb:
    # This(EncryptedFileSystem) is for TDE encryption for NDBMTD data
nodes
    # The files in the data nodes are encrypted which store the
subscriber and configuration data which may contains sensitive
information.
    EncryptedFileSystem: 0

db-replication-svc:
  numberofparallelbackuptransfer: 4
    validateresourcesingeorecovery: true
```

   c. The values of following configuration have been changed:

```
global:
  additionalndbconfigurations:
    ndb:
      HeartbeatIntervalDbDb:1250
    api:
      binlogpurgetimer:600s
db-replication-svc:
  dbreplsvcdeployments:
```

```
      - name: cndbtiersitename-cndbtierfirstmatesitename-replication-svc
        schedulertimer: "5s"
      - name: cndbtiersitename-cndbtiersecondmatesitename-replication-svc
        schedulertimer: "5s"
      - name: cndbtiersitename-<${OCCNE_THIRD_MATE_SITE_NAME}>-
replication-svc
        schedulertimer: "5s"

db-monitor-svc:
  schedulertimer: "5s"
  metricsFetchSchedulerTimer: "55s"
```

5. **IAM KC Log Level Change**
   By default, the log level of M-CNCC IAM KC is set to **WARN,org.keycloak.events:DEBUG**

   This means the root log-level for is set to **WARN** and the org.kecyalok.events package is set to **DEBUG**.

```
kc:
 log:
   level: WARN,org.keycloak.events:DEBUG
```

6. **Configuring M-CNCC IAM to enable additional settings**
   CNC Console provides the option to enable additional settings in M-CNCC IAM. To enable additional settings in M-CNCC IAM, the following flag must be enabled in the `occncc_custom_values_<version>.yaml` file.

   The additional settings include:

   - Realm Settings to configure Require SSL and token configuration
   - Authentication settings to configure password policies Session setting

```
cncc-iam:
  global:
    iamSettingEnabled: false
```

7. **Security Context Constraint changes**

   a. **Security Context Constraint are introduced at global level and at each services**

```
##############################################################
#            Section Start: global attributes           #
##############################################################
global:
  enablePodSecurityContext: &enablePodSecurityContext true
  podSecurityContext:
    runAsNonRoot: &runAsNonRootPod true
    runAsUser: &runAsUserPod 1006

  enableContainerSecurityContext: &enableContainerSecurityContext true
  containerSecurityContext:
    readOnlyRootFilesystem: &readOnlyRootFilesystem true
    allowPrivilegeEscalation: &allowPrivilegeEscalation false
    runAsNonRoot: &runAsNonRootContainer true
    privileged: &privileged false
```

```
    runAsUser: &runAsUser 1006
    capabilities: &capabilities
      drop:
        - "ALL"

  validationHook:
    enableContainerSecurityContext: *enableContainerSecurityContext
    containerSecurityContext:
      readOnlyRootFilesystem: *readOnlyRootFilesystem
      allowPrivilegeEscalation: *allowPrivilegeEscalation
      runAsNonRoot: *runAsNonRootContainer
      privileged: *privileged
      runAsUser: *runAsUser
      capabilities: *capabilities
#####################################################################
#            Section Start  : cncc iam attributes            #
#####################################################################

cncc-iam:
    hook:
      enableContainerSecurityContext: *enableContainerSecurityContext
      containerSecurityContext:
        readOnlyRootFilesystem: false
        allowPrivilegeEscalation: *allowPrivilegeEscalation
        runAsNonRoot: *runAsNonRootContainer
        privileged: *privileged
        runAsUser: *runAsUser
        capabilities: *capabilities
  kc:
    enablePodSecurityContext: *enablePodSecurityContext
    podSecurityContext:
      runAsNonRoot: *runAsNonRootPod
      runAsUser: 1000

    healthcheck:
      enableContainerSecurityContext: *enableContainerSecurityContext
      containerSecurityContext:
        readOnlyRootFilesystem: false
        allowPrivilegeEscalation: *allowPrivilegeEscalation
        runAsNonRoot: *runAsNonRootContainer
        privileged: *privileged
        runAsUser: *runAsUser
        capabilities: *capabilities

    keycloak:
      enableContainerSecurityContext: *enableContainerSecurityContext
      containerSecurityContext:
        readOnlyRootFilesystem: false
        allowPrivilegeEscalation: *allowPrivilegeEscalation
        runAsNonRoot: *runAsNonRootContainer
        privileged: *privileged
        runAsUser: 1000
        capabilities: *capabilities
#############################################################################
#            Section Start  : manager cncc core attributes            #
#############################################################################
```

```
    mcncc-core:
      cmservice:
        enablePodSecurityContext: *enablePodSecurityContext
        podSecurityContext:
          runAsNonRoot: *runAsNonRootPod
          runAsUser: *runAsUserPod
        enableContainerSecurityContext: *enableContainerSecurityContext
        containerSecurityContext:
          readOnlyRootFilesystem: false
          allowPrivilegeEscalation: *allowPrivilegeEscalation
          runAsNonRoot: *runAsNonRootContainer
          privileged: *privileged
          runAsUser: *runAsUser
          capabilities: *capabilities
```

b. **Security Context Constraint is modified for extra containers** (runAsUser 7000 is added)

```
global:
  extraContainers: DISABLED
  ...
  ...
  extraContainersTpl: |
    ...
    ...
      securityContext:
        allowPrivilegeEscalation: true
        capabilities:
          drop:
          - ALL
          add:
          - NET_RAW
          - NET_ADMIN
        runAsUser: 7000
```

4.2 REST API

This section lists the REST API changes in release 24.3.x. For more information about the REST APIs, see *Oracle Communications Cloud Native Configuration Console REST Specifications Guide.*

Release 24.3.0

There are no changes in the REST API in this release.

4.3 CNC Console

This section lists the CNC Console changes in release 24.3.x. For more information about the CNC Console configurations, see *Oracle Communications Cloud Native Configuration Console User Guide.*

Release 24.3.0

There are no changes in the CNC Console in this release.

5 Observability

This chapter lists the observability changes in release 24.3.x.

5.1 Metrics

This section lists the added or updated metrics in release 24.3.x. For more information on the metrics, see *Oracle Communications Cloud Native Configuration Console User Guide.*

Release 24.3.0
There are no updates to metrics in this release.

5.2 Alerts

This section lists the added or updated alerts in release 24.3.x. For more information on the Alerts, see *Oracle Communications Cloud Native Configuration Console User Guide.*

Release 24.3.0

There are no updates to alerts in this release.

5.3 KPIs

This section lists the added or updated KPIs in release 24.3.x. For more information on the KPIs, see *Oracle Communications Cloud Native Configuration Console User Guide.*

Release 24.3.0

There are no updates to KPIs in this release.