Oracle® Communications

Oracle Communications Networks Data Analytics Function Troubleshooting Guide

Release 22.0.0
F70774-01
October 2022

Oracle Communications Oracle Communications Networks Data Analytics Function Troubleshooting Guide, Release 22.0.0

F70774-01

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 provides information about the acronyms and the terminology used in the document.

Table Acronyms

Acronym	Description
3GPP	3rd Generation Partnership Project
5GC	5G Core Network
5GS	5G System
AF	Application Function
API	Application Programming Interface
AMF	Access and Mobility Management Function
AnLF	Analytics Logical Function
CAP4C	Converged Analytics Platform for Communication
CNC	Cloud Native Core
CNE	Cloud Native Environment
CSP	Communications Service Provider
FE	Front End
FQDN	Fully Qualified Domain Name
GUI	Graphical User Interface
HTTPS	Hypertext Transfer Protocol Secure
KPI	Key Performance Indicator
HA	High Availability
IMSI	International Mobile Subscriber Identity
K8s	Kubernetes
MDT	Mobile Data Terminal
ME	Monitoring Events
MICO	Mobile Initiated Connection Only
ML	Machine Learning
MLOPs	Machine Learning Operations
MTLF	Model Training Logical Function
Network Slice	A logical network that provides specific network capabilities and network characteristics.
NEF	Network Exposure Function
NF	Network Function
NRF	Network Repository Function
NSI	Network Slice instance. A set of Network Function instances and the required resources (such as compute, storage and networking resources) which form a deployed Network Slice.
NSSF	Network Slice Selection Function
OCNWDAF	Oracle Communications Networks Data Analytics Function
OAM	Operations, Administration, and Maintenance
PLMN	Public Land Mobile Network

Table (Cont.) Acronyms

Acronym	Description
RAN	Radio Access Network
REST	Representational State Transfer
SBA	Service Based Architecture
SBI	Service Based Interface
SMF	Session Management Function
SNMP	Simple Network Management Protocol
SUPI	Subscription Permanent Identifier
UDM	Unified Data Management
UE	User Equipment
UPF	User Plane Function
UDR	Unified Data Repository
UDM	Unified Data Management
URI	Uniform Resource Identifier

What's New in This Guide

This section introduces the documentation updates for Release 22.0.0 in Oracle Communications Networks Data Analytics Function Troubleshooting Guide.

Release 22.0.0 - F70774-01, October 2022

This is the first published version of the document.

1
Introduction

This document provides information about troubleshooting Oracle Communications Network Data Analytics Function (OCNWDAF).

1.1 Overview

Oracle Communications Network Data Analytics Function (OCNWDAF) is a Network Function (NF) in the 5G core network of the 5G Network Architecture.

The OCNWDAF enables the operator to collect and analyze the data in the network through an analytics function. The 5G technology requires prescriptive analytics to drive closed-loop automation and self-healing networks. In a 5G network, the consumers of data are 5G NFs, Application Functions (AFs), and Operations, Administration, and Maintenance (OAM) and the data producers are NFs.

1.2 Audience

The intended audiences for this document are the network administrators and the professionals responsible for OCNWDAF deployment and maintenance.

1.3 References

For more information about OCNWDAF, refer to the following documents:

- *Oracle Communications Networks Data Analytics Function Installation Guide*
- *Oracle Communications Networks Data Analytics Function User Guide*
- *Oracle Communications Networks Data Analytics Function Solution Guide*
- *Oracle Communications Networks Data Analytics Function Disaster Recovery Guide*
- *Oracle Communications Cloud Native Environment Installation Guide*

2
Logs

This chapter explains the process to retrieve the logs and status that can be used for effective troubleshooting.

2.1 Log Levels

Logs register system events along with their date and time of occurrence. They also provide important details about a chain of events that could have led to an error or problem.

A log level helps in defining the severity level of a log message. For OCNWDAF, the log level of a microservice can be set to any one of the following valid values:

- **TRACE**: A log level that describes events, as a step by step execution of code. This can be ignored during the standard operation, but may be useful during extended debugging sessions.
- **DEBUG**: A log level used for events during software debugging when more granular information is needed.
- **INFO**: A standard log level indicating that something has happened, an application has entered a certain state, etc.
- **WARN**: A log level indicates that something unexpected has happened in the application, a problem, or a situation that might disturb one of the processes. But this does not mean that the application has failed. The WARN level should be used in situations that are unexpected, but the code can continue to work.
- **ERROR**: A log level that should be used when an application hits an issue preventing one or more functionalities from functioning.

> **Note:**
>
> Log levels are defined in the helm chart and as parameters of the Kubernetes pod, they can be updated by changing the Kubernetes pod deployment.

Using this information, the logs can be filtered based on the system requirements. For instance, if you want to filter the critical information about your system from the informational log messages, set a filter to view messages with only WARN log level in Kibana.

The following table provides log level details that may be helpful to handle different OCNWDAF debugging issues:

Table 2-1 Log Levels

Scenarios	Pod	Logs to be searched	Log Level
Registration with NRF Successful	nrf-client-service	Register completed successfully / "nfServiceStatus":"REGISTERED"	INFO
Heartbeat message log	nrf-client-service	Update completed successfully	INFO
NRF configurations reloading	nrf-client-service	NRF client config reloaded	INFO
Check for exiting NF Instance Entry	nrf-client-service	No registered NF instance exists	WARN
Started Application	nrf-client-service	Successful application start	INFO
NRF Client Config Initialized	nrf-client-service	Initialize NRF client configuration	INFO
FQDN/BASEURL/ livenessProbeUrl Improper	nrf-client-service	response=<503,java.net.UnknownHostException	WARN
nudr-drservice liveness probe failure	nrf-client-service	NFService liveness probe failed	WARN
Check if Ports successfully listening	nrf-client-service	Undertow started on port(s)	INFO
Registration with NRF failed	nrf-client-service	Register failed	ERROR
De registration with NRF successful	nrf-client-service	Deregister completed successfully	INFO
De registration with NRF failed	nrf-client-service	Deregister failed	ERROR
NF Profile update failed	nrf-client-service	Update failed	ERROR

2.2 Collecting Logs

This section describes the steps to collect logs from PODs and containers. Perform the following steps:

1. Run the following command to get the PODs details:

   ```
   kubectl -n <namespace_name> get pods
   ```

2. Collect the logs from the specific pods or containers:

   ```
   kubectl logs <podname> -n <namespace> -c <containername>
   ```

3. Store the log in a file using the following command:

   ```
   kubectl logs <podname> -n <namespace> > <filename>
   ```

4. (Optional) You can also use the following commands for the log stream with file redirection starting with last 100 lines of log:

```
kubectl logs <podname> -n <namespace> -f --tail <number of lines> >
<filename>
```

For more information on how to collect the logs, see *Oracle Communication Cloud Native Core Data Collector Guide*.

2.3 Understanding Logs

This chapter explains the logs you need to look into to handle different OCNWDAF debugging issues.

For more information on how to collect the logs, see *Oracle Communication Cloud Native Core Data Collector Guide*.

Log Formats

The following log formats are supported:

- **Executor logs**
  Format:

  ```
  <datetime> - <level> - <module>.<line> [<thread>] : <message>
  ```

  Where:

  - `datetime` - The date and time of the event.
  - `level` - Helps in defining the severity level of a log message.
  - `module` - Software component that created the message.
  - `line` - Line of the source code where the message happened.
  - `thread` - Name of the thread that was currently executing.
  - `message` - Description of the event.
- **Controller logs**
  Format:

  ```
  <datetime>  <level> <process> --- [<thread>] <loggername> : <message>
  ```

  Where:

  - `datetime` - The date and time of the event.
  - `level` - Helps in defining the severity level of a log message.
  - `process` - Name of the process that was currently executing.
  - `thread` - Name of the thread that was currently executing.
  - `loggername` - The source class name (often abbreviated).
  - `message` - Description of the event.

3
Using Debug Tool

The Debug Tool provides third-party troubleshooting tools for debugging the runtime issues for the lab and production environment. The following tools are available for OCNWDAF debugging:

- tcpdump
- ip
- netstat
- curl
- ping
- nmap
- dig

Preconfiguration Steps

This section explains the preconfiguration steps for using the debug tool:

1. **Configuration in CNE**
   The following configurations must be performed in the Bastion Host.

   PodSecurityPolicy (PSP) Creation

   a. Log in to the Bastion Host.

   b. Create a new PSP by running the following command from the bastion host. The parameters `readOnlyRootFileSystem`, `allowPrivilegeEscalation`, `allowedCapabilities` are required by debug container.

> **Note:**
>
> Other parameters are mandatory for PSP creation and can be customized as per the CNE environment. Default values are recommended.

```
$ kubectl apply -f - <<EOF

apiVersion: policy/v1beta1
kind: PodSecurityPolicy
metadata:
  name: debug-tool-psp
spec:
  readOnlyRootFilesystem: false
  allowPrivilegeEscalation: true
  allowedCapabilities:
  - NET_ADMIN
  - NET_RAW
```

```
  fsGroup:
    ranges:
    - max: 65535
      min: 1
    rule: MustRunAs
  runAsUser:
    rule: MustRunAsNonRoot
  seLinux:
    rule: RunAsAny
  supplementalGroups:
    rule: RunAsAny
  volumes:
  - configMap
  - downwardAPI
  - emptyDir
  - persistentVolumeClaim
  - projected
  - secret
EOF
```

Role Creation

Run the following command to create a role for the PSP:

```
kubectl apply -f - <<EOF
apiVersion: rbac.authorization.k8s.io/v1
kind: Role
metadata:
  name: debug-tool-role
  namespace: cncc
rules:
- apiGroups:
  - policy
  resources:
  - podsecuritypolicies
  verbs:
  - use
  resourceNames:
  - debug-tool-psp
EOF
```

RoleBinding Creation

Run the following command to attach the service account for your NF namespace with the role created for the tool PSP:

```
$ kubectl apply -f - <<EOF
apiVersion: rbac.authorization.k8s.io/v1
kind: RoleBinding
metadata:
  name: debug-tool-rolebinding
  namespace: ocnef
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: Role
```

```
  name: debug-tool-role
subjects:
- kind: Group
  apiGroup: rbac.authorization.k8s.io
  name: system:serviceaccounts
EOF
```

2. Configuration in NF specific Helm
   Following updates must be performed in custom_values.yaml file.
   a. Log in to the NF server.
   b. Open the custom_values file:

      ```
      $ vim <custom_values file>
      ```

   c. Under global configuration, add the following:

      ```
      # Allowed Values: DISABLED, ENABLED
      extraContainers: DISABLED
      extraContainersTpl: |
          - command:
              - /bin/sleep
              - infinity
            image: <image-name>:<image-tag>
            imagePullPolicy: Always
            name: tools
            resources:
              requests:
                ephemeral-storage: "2Gi"
                cpu: "0.5"
                memory: "1Gi"
              limits:
                ephemeral-storage: "4Gi"
                cpu: "1"
                memory: "2Gi"
            securityContext:
              allowPrivilegeEscalation: true
              capabilities:
                drop:
                - ALL
                add:
                - NET_RAW
                - NET_ADMIN
              readOnlyRootFilesystem: false
              runAsUser: <user>
      ```

> **Note:**
>
> - Debug Tool Container comes up with the default user ID - 7000. If the operator wants to override this default value, it can be done using the `runAsUser` field, otherwise, the field can be skipped. Default value: uid=7000(debugtool) gid=7000(debugtool) groups=7000(debugtool)
> - In case you want to customize the container name, replace the `name` field in the above values.yaml with the following:
>
>   ```
>   name: {{ printf "%s-tools-%s" (include
>   "getprefix" .) (include "getsuffix" .) | trunc 63 |
>   trimPrefix "-" | trimSuffix "-"  }}
>   ```
>
>   This will ensure that the container name is prefixed and suffixed with the necessary values.

d. Under service specific configurations for which debugging is required, add the following:

```
# Allowed Values: DISABLED, ENABLED, USE_GLOBAL_VALUE
extraContainers: USE_GLOBAL_VALUE
```

> **Note:**
>
> - – At the global level, `extraContainers` flag can be used to enable/disable injecting extra containers globally. This ensures that all the services that use this global value have extra containers enabled/disabled using a single flag.
> - – At the service level, `extraContainers` flag determines whether to use the extra container configuration from the global level or enable/disable injecting extra containers for the specific service.

Run the Debug Tool

Following is the procedure to run Debug Tool.

Run the following command to enter Debug Tool Container:

1. Run the following command to retrieve the POD details:

   ```
   $ kubectl get pods -n <k8s namespace>
   ```

2. Run the following command to enter Debug Tool Container:

   ```
   $ kubectl exec -it <pod name> -c <debug_container name> -n
   <namespace> -- bash
   ```

3. Run the debug tools:

```
bash -4.2$ <debug_tools>
```

4. Copy the output files from container to host:

```
$ kubectl cp -c <debug_container name> <pod name>:<file location in
container> -n <namespace> <destination location>
```

3.1 Debug Tool Configuration Parameters

Following are the parameters used to configure debug tool.

OCCNE Parameters

Table 3-1 OCCNE Parameters

Parameter	Description
apiVersion	APIVersion defines the version schema of this representation of an object.
kind	Kind is a string value representing the REST resource this object represents.
metadata	Standard object's metadata.
metadata.name	Name must be unique within a namespace.
spec	spec defines the policy enforced.
spec.readOnlyRootFilesystem	Controls whether the containers run with a read-only root filesystem (that is, no writable layer).
spec.allowPrivilegeEscalation	Gates whether or not a user is allowed to set the security context of a container to allowPrivilegeEscalation=true.
spec.allowedCapabilities	Provides a list of capabilities that are allowed to be added to a container.
spec.fsGroup	Controls the supplemental group applied to some volumes. RunAsAny allows any fsGroup ID to be specified.
spec.runAsUser	Controls which user ID the containers are run with. RunAsAny allows any runAsUser to be specified.
spec.seLinux	RunAsAny allows any seLinuxOptions to be specified.
spec.supplementalGroups	Controls which group IDs containers add. RunAsAny allows any supplementalGroups to be specified.
spec.volumes	Provides a list of allowed volume types. The allowable values correspond to the volume sources that are defined when creating a volume.

Role Creation Parameters

Table 3-2 Role Creation

Parameter	Description
apiVersion	APIVersion defines the versioned schema of this representation of an object.
kind	Kind is a string value representing the REST resource this object represents.
metadata	Standard object's metadata.
metadata.name	Name must be unique within a namespace.
metadata.namespace	Namespace defines the space within which each name must be unique.
rules	Rules holds all the PolicyRules for this Role
apiGroups	APIGroups is the name of the APIGroup that contains the resources.
rules.resources	Resources is a list of resources this rule applies to.
rules.verbs	Verbs is a list of Verbs that apply to ALL the ResourceKinds and AttributeRestrictions contained in this rule.
rules.resourceNames	ResourceNames is an optional allowed list of names that the rule applies to.

Role Binding Creation

Table 3-3 Role Binding Creation

Parameter	Description
apiVersion	APIVersion defines the versioned schema of this representation of an object.
kind	Kind is a string value representing the REST resource this object represents.
metadata	Standard object's metadata.
metadata.name	Name must be unique within a namespace.
metadata.namespace	Namespace defines the space within which each name must be unique.
roleRef	RoleRef can reference a Role in the current namespace or a ClusterRole in the global namespace.
roleRef.apiGroup	APIGroup is the group for the resource being referenced
roleRef.kind	Kind is the type of resource being referenced
roleRef.name	Name is the name of resource being referenced
subjects	Subjects holds references to the objects the role applies to.
subjects.kind	Kind of object being referenced. Values defined by this API group are "User", "Group", and "ServiceAccount".
subjects.apiGroup	APIGroup holds the API group of the referenced subject.
subjects.name	Name of the object being referenced.

Debug Tool Configuration Parameters

Table 3-4 Debug Tool Configuration Parameters

Parameter	Description
command	String array used for container command.
image	Docker image name
imagePullPolicy	Image Pull Policy
name	Name of the container
resources	Compute Resources required by this container
resources.limits	Limits describes the maximum amount of compute resources allowed
resources.requests	Requests describes the minimum amount of compute resources required
resources.limits.cpu	CPU limits
resources.limits.memory	Memory limits
resources.limits.ephemeral-storage	Ephemeral Storage limits
resources.requests.cpu	CPU requests
resources.requests.memory	Memory requests
resources.requests.ephemeral-storage	Ephemeral Storage requests
securityContext	Security options the container should run with.
securityContext.allowPrivilegeEscalation	AllowPrivilegeEscalation controls whether a process can gain more privileges than its parent process. This directly controls if the no_new_privs flag will be set on the container process
securityContext.readOnlyRootFilesystem	Whether this container has a read-only root filesystem. Default is false.
securityContext.capabilities	The capabilities to add/drop when running containers. Defaults to the default set of capabilities granted by the container runtime.
securityContext.capabilities.drop	Removed capabilities
securityContext.capabilities.add	Added capabilities
securityContext.runAsUser	The UID to run the entrypoint of the container process.

4
Troubleshooting OCNWDAF

This chapter provides information to troubleshoot the common errors which can be encountered during the preinstallation, installation, upgrade, and rollback procedures of OCNWDAF.

4.1 Generic Checklist

The following sections provide a generic checklist for troubleshooting tips.

Deployment related tips

Perform the following checks after the deployment:

- Are OCNWDAF deployment, pods, and services created?
  Are OCNWDAF deployment, pods, and services running and available?

  Run the following the command:

  ```
  # kubectl -n <namespace> get deployments,pods,svc
  ```

  Inspect the output, check the following columns:

  – AVAILABLE of deployment
  – READY, STATUS, and RESTARTS of a pod
  – PORT(S) of service
- Check if the microservices can access each other via REST interface.
  Run the following command:

  ```
  # kubectl -n <namespace> exec <pod name> -- curl <uri>
  ```

Application related tips

Run the following command to check the application logs and look for exceptions:

```
# kubectl -n <namespace> logs -f <pod name>
```

You can use '-f' to follow the logs or 'grep' for specific pattern in the log output.

4.2 Deployment Related Issue

This section describes the most common deployment related issues and their resolution steps. It is recommended to perform the resolution steps provided in this guide. If the issue still persists, then contact My Oracle Support.

4.2.1 Installation

This section describes the most common installation related issues and their resolution steps.

- Pod Creation Failure
- Pod Startup Failure
- NRF Registration Failure

4.2.1.1 Pod Creation Failure

A pod creation can fail due to various reasons. Some of the possible scenarios are as follows:

Verifying Pod Image Correctness

To verify pod image:

- Check whether any of the pods is in the **ImagePullBackOff** state.
- Check if the image name used for all the pods are correct. Verify the image names and versions in the OCNWDAF installation file. For more information about the custom value file, see *Oracle Communications Networks Data Analytics Function Installation Guide*.

Verifying Resource Allocation Failure

To verify any resource allocation failure:

- Run the following command to verify whether any pod is in the pending state.
  `kubectl describe <nwdaf-drservice pod id> --n <ocnef-namespace>`
- Verify whether any warning on insufficient CPU exists in the describe output of the respective pod. If it exists, it means there are insufficient CPUs for the pods to start. Address this hardware issue.

Verifying Resource Allocation Issues on Webscale Environment

Webscale environment has openshift container installed. There can be cases where,

- Pods does not scale after you run the installation command and the installation fails with timeout error. In this case, check for preinstall hooks failure. Run the **oc get job** command to create the jobs. Describe the job for which the pods are not getting scaled and check if there are **quota limit exceeded** errors with CPU or memory.
- Any of the actual microservice pods do not scale post the hooks completion. In this case, run the **oc get rs** command to get the list of replicaset created for the NF deployment. Then, describe the replicaset for which the pods are not getting scaled and check for **resource quota limit exceeded** errors with CPU or memory.
- Installation times-out after all the microservice pods are scaled as expected with the expected number of replicas. In this case, check for post install hooks failure. Run the **oc get job** command to get the post install jobs and do a describe on the job for which the pods are not getting scaled and check if there are **quota limit exceeded** errors with CPU or memory.

- Resource quota exceed beyond limits.

4.2.1.2 Pod Startup Failure

Follow the guidelines shared below to debug the pod startup failure liveness check issues:

- If dr-service, diameter-proxy, and diam-gateway services are stuck in the Init state, then the reason could be that config-server is not yet up. A sample log on these services is as follows:

  ```
  "Config Server is Not yet Up, Wait For config server to be up."
  ```

  To resolve this, you must either check for the reason of config-server not being up or if the config-server is not required, then disable it.
- If the notify and on-demand migration service is stuck in the Init state, then the reason could be the dr-service is not yet up. A sample log on these services is as follows:

  ```
  "DR Service is Not yet Up, Wait For dr service to be up."
  ```

  To resolve this, check for failures on dr-service.

4.2.1.3 NRF Registration Failure

The OCNWDAF registration with NRF may fail due to various reasons. Some of the possible scenarios are as follows:

- Confirm whether registration was successful from the nrf-client-service pod.
- Check the ocnwdaf-nrf-client-nfmanagement logs. If the log has **"OCNWDAF is Unregistered"** then:
  - Check if all the services mentioned under allorudr/slf (depending on OCNWDAF mode) in the installation file has same spelling as that of service name and are enabled.
  - Once all services are up, OCNWDAF must register with NRF.
- If you see a log for **SERVICE_UNAVAILABLE(503)**, check if the primary and secondary NRF configurations (primaryNrfApiRoot/secondaryNrfApiRoot) are correct and they are UP and Running.

4.3 Database Related Issues

This section describes the most common database related issues and their resolution steps. It is recommended to perform the resolution steps provided in this guide. If the issue still persists, then contact My Oracle Support.

4.3.1 Debugging MySQL DB Errors

If you are facing issues related to subscription creation, follow the procedure below to login to MySQL DB:

> **Note:**
>
> Once the MySQL cluster is created, the *cndbtier_install container* generates the password and stores it in the *occne-mysqlndb-root-secret* secret.

1. Retrieve the MySQL root password from *occne-mysqlndb-root-secret* secret. Run the command:

   ```
   $ kubectl -n occne-cndbtier get secret occne-mysqlndb-root-secret -
   o jsonpath='{.data}'map[mysql_root_password:TmV4dEdlbkNuZQ==]
   ```

2. Decode the encoded output received as an output of the previous step to get the actual password:

   ```
   $ echo TmV4dEdlbkNuZQ== | base64 --decode
   NextGenCne
   ```

3. Login to MySQL pod, run the command:

   ```
   $ kubectl -n occnepsa exec -it ndbmysqld-0 -- bash
   ```

   > **Note:**
   >
   > Default container name is: `mysqlndbcluster`.
   > Run the command `kubectl describe pod/ndbmysqld-0 -n occnepsa` to see all the containers in this pod.

4. Login using MySQL client as the root user, run the command:

   ```
   $ mysql -h 127.0.0.1 -uroot -p
   ```

5. Enter current root password for MySQL root user obtained from step 2.
6. To debug each microservice, perform the following steps:
   - For the **ocn-nwdaf-subscription** service, run the following SQL commands:

     ```
     use <dbName>;
     use nwdaf_subscription;
     select * from nwdaf_subscription;
     select * from amf_ue_event_subscription
     select * from smf_ue_event_subscription
     ```

   - For the **ocn-nrf-simulator** service, run the following SQL commands:

     ```
     use <dbName>;
     use nrf;
     select * from profile;
     ```

- For the **ocn-smf-simulator** service, run the following SQL commands:

```
use <dbName>;
use nrf;
select * from smf_event_subscription;
```

- For the **ocn-amf-simulator** service, run the following SQL commands:

```
use <dbName>;
use nrf;
select * from amf_event_subscription;
```

- For the **ocn-nwdaf-data-collection** service, run the following SQL commands:

```
use <dbName>;
use nwdaf_data_collection;
select * from amf_event_notification_report_list;
select * from amf_ue_event_report;
select * from cap4c_ue_notification;
select * from slice_load_level_notification;
select * from smf_event_notification_report_list;
select * from smf_ue_event_report;
select * from ue_mobility_notification;
```

- For the **ocn-nwdaf-configuration-service** service, run the following SQL commands:

```
use <dbName>;
use nwdaf_configuration_service;
select * from slice;
select * from tracking_are;
select * from slice_tracking_area;
select * from cell;
```

4.4 Apache Kafka Related Issues

To debug issues related to Apache Kafka pipelines (such as, unable to read messages from the pipeline or write messages to the pipeline) perform the following steps:

1. Get the Kafka pods, run the command:

```
kubectl -n performance-ns get pods -o wide | grep "kafka"
```

2. Select any pod and access the pod using the command:

```
kubectl -n performance-ns exec -it kafka-sts-0 -- bash
```

3. Move to the directory containing the binary files, run the command:

```
cd kafka_2.13-3.1.0/bin/
```

4. Obtain the list of topics, run the command:

```
kafka-topics.sh --list --bootstrap-server localhost:9092
```

5. For each topic, run the following command:

```
kafka-console-consumer.sh --bootstrap-server 127.0.0.1:9092 --topic
    <topic-name>
```

4.5 CAP4C Related Issues

CAP4C comprises of the following services:

- cap4c-model-controller
- cap4c-model-executor
- druid-pod
- kafka
- mysql-pod

To obtain more information on the service pods, follow the steps listed below:

1. Each of these services is deployed as pod in Kubernetes. To find the status of the pods in Kubernetes run the following command:

```
$ kubectl get pods -n <namespace>
```

Sample output:

```
NAME                                                    READY
STATUS    RESTARTS   AGE

cap4c-model-controller-deploy-779cbdcf8f-w2pfh          1/1
Running   0          4d8h

cap4c-model-executor-deploy-f9c96db54-ttnhd             1/1
Running   0          4d5h

cap4c-stream-analytics-deploy-744878569-5xr2w           1/1
Running   0          4d8h

druid-pod                                               1/1
Running   0          4d8h
```

2. To verify the pod information, print the detail of each pod to:

```
$ kubectl describe pod cap4c-model-controller-deploy-779cbdcf8f-
w2pfh  -n
    <namespace>
```

Sample output:

```
Name:         cap4c-model-controller-deploy-779cbdcf8f-w2pfh

Namespace:    performance-ns

Priority:     0

Node:         sunstreaker-k8s-node-2/192.168.200.197

Start Time:   Fri, 26 Aug 2022 15:31:39 +0000

Labels:       app=cap4c-model-controller

              pod-template-hash=779cbdcf8f

Annotations:  cni.projectcalico.org/containerID:
480ca581a828184ccf6fabf7ec7cfb68920624f48d57148f6d93db4512bc5335

              cni.projectcalico.org/podIP: 10.233.76.134/32

              cni.projectcalico.org/podIPs: 10.233.76.134/32

              kubernetes.io/psp: restricted

              seccomp.security.alpha.kubernetes.io/pod: runtime/default

Status:       Running
```

3. List the service configuration for the pods, run the command:

```
$ kubectl get svc -n <namespace>
```

Sample output:

```
NAME              TYPE        CLUSTER-IP      EXTERNAL-IP
         PORT(S)    AGE cap4c-executor    ClusterIP   10.233.5.218
<none>
        8080/TCP   4d8h druid             ClusterIP   10.233.10.167
<none>
        8888/TCP   4d8h druid-svc         NodePort    10.233.39.96
<none>
        8888:32767/TCP 4d8h
```

4.6 Service Related Issues

This section describes the most common service related issues and their resolution steps. It is recommended to perform the resolution steps provided in this guide. If the issue still persists, then contact My Oracle Support.

4.6.1 Errors from Microservices

The OCNWDAF microservices are listed below:

- ocn-nwdaf-subscription
- ocn-nwdaf-data-collection
- ocn-nwdaf-communication
- ocn-nwdaf-configuration-service
- ocn-nwdaf-analytics
- ocn-nwdaf-gateway
- ocn-nwdaf-mtlf
- ocn-nrf-simulator
- ocn-smf-simulator
- ocn-amf-simulator
- mesa-simulator

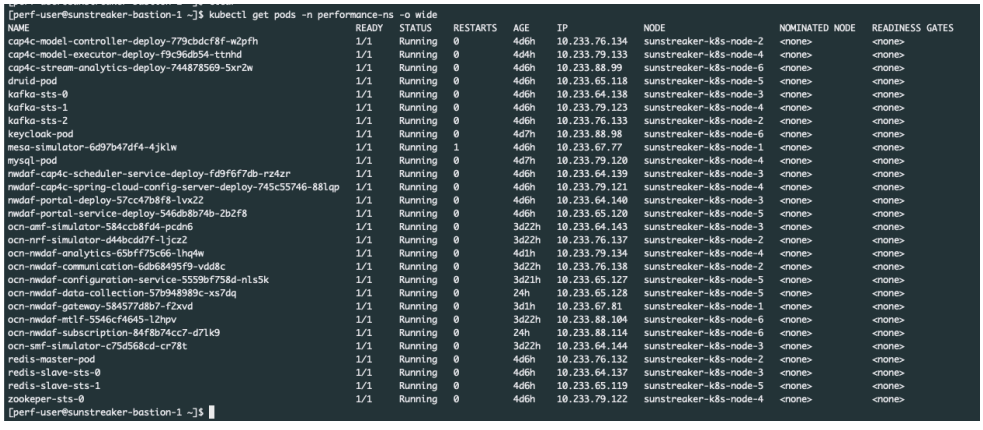
To debug microservice related errors, obtain the logs in the pods which are facing issues, run the following commands for each microservice:

1. Obtain the pod information, run the command:

   ```
   kubectl get pods -n <nameSpace> -o wide
   ```

   Sample output:

   Figure 4-1 Pod Information



```
[perf-user@sunstreaker-bastion-1 ~]$ kubectl get pods -n performance-ns -o wide
NAME                                                  READY   STATUS    RESTARTS   AGE    IP              NODE                      NOMINATED NODE   READINESS GATES
cap4c-model-controller-deploy-779cbdcf8f-w2pfh        1/1     Running   0          4d6h   10.233.76.134   sunstreaker-k8s-node-2    <none>           <none>
cap4c-model-executor-deploy-f9c96db54-ttnhd           1/1     Running   0          4d4h   10.233.79.133   sunstreaker-k8s-node-4    <none>           <none>
cap4c-stream-analytics-deploy-744878569-5xr2w         1/1     Running   0          4d6h   10.233.88.99    sunstreaker-k8s-node-6    <none>           <none>
druid-pod                                             1/1     Running   0          4d6h   10.233.65.118   sunstreaker-k8s-node-5    <none>           <none>
kafka-sts-0                                           1/1     Running   0          4d6h   10.233.64.138   sunstreaker-k8s-node-3    <none>           <none>
kafka-sts-1                                           1/1     Running   0          4d6h   10.233.79.123   sunstreaker-k8s-node-4    <none>           <none>
kafka-sts-2                                           1/1     Running   0          4d6h   10.233.76.133   sunstreaker-k8s-node-2    <none>           <none>
keycloak-pod                                          1/1     Running   0          4d7h   10.233.88.98    sunstreaker-k8s-node-6    <none>           <none>
mesa-simulator-6d97b47df4-4jklw                       1/1     Running   1          4d6h   10.233.67.77    sunstreaker-k8s-node-1    <none>           <none>
mysql-pod                                             1/1     Running   0          4d7h   10.233.79.120   sunstreaker-k8s-node-4    <none>           <none>
nwdaf-cap4c-scheduler-service-deploy-fd9f6f7db-rz4zr  1/1     Running   0          4d6h   10.233.64.139   sunstreaker-k8s-node-3    <none>           <none>
nwdaf-cap4c-spring-cloud-config-server-deploy-745c55746-88lqp  1/1     Running   0          4d6h   10.233.79.121   sunstreaker-k8s-node-4    <none>           <none>
nwdaf-portal-deploy-57cc47b8f8-lvx22                  1/1     Running   0          4d6h   10.233.64.140   sunstreaker-k8s-node-3    <none>           <none>
nwdaf-portal-service-deploy-546db8b74b-2b2f8          1/1     Running   0          4d6h   10.233.65.120   sunstreaker-k8s-node-5    <none>           <none>
ocn-amf-simulator-584ccb8fd4-pcdn6                    1/1     Running   0          3d22h  10.233.64.143   sunstreaker-k8s-node-3    <none>           <none>
ocn-nrf-simulator-d44bcdd7f-ljcz2                     1/1     Running   0          3d22h  10.233.76.137   sunstreaker-k8s-node-2    <none>           <none>
ocn-nwdaf-analytics-65bff75c66-lhq4w                  1/1     Running   0          4d1h   10.233.79.134   sunstreaker-k8s-node-4    <none>           <none>
ocn-nwdaf-communication-6db68495f9-vdd8c              1/1     Running   0          3d22h  10.233.76.138   sunstreaker-k8s-node-2    <none>           <none>
ocn-nwdaf-configuration-service-55598bf758d-nls5k     1/1     Running   0          3d21h  10.233.65.127   sunstreaker-k8s-node-5    <none>           <none>
ocn-nwdaf-data-collection-57b948989c-xs7dq            1/1     Running   0          24h    10.233.65.128   sunstreaker-k8s-node-5    <none>           <none>
ocn-nwdaf-gateway-584577d8b7-f2xvd                    1/1     Running   0          3d1h   10.233.67.81    sunstreaker-k8s-node-1    <none>           <none>
ocn-nwdaf-mtlf-5546cf4645-lzhpv                       1/1     Running   0          3d22h  10.233.88.104   sunstreaker-k8s-node-6    <none>           <none>
ocn-nwdaf-subscription-84f8b74cc7-d7lk9               1/1     Running   0          24h    10.233.88.114   sunstreaker-k8s-node-6    <none>           <none>
ocn-smf-simulator-c75d568cd-cr78t                     1/1     Running   0          3d22h  10.233.64.144   sunstreaker-k8s-node-3    <none>           <none>
redis-master-pod                                      1/1     Running   0          4d6h   10.233.76.132   sunstreaker-k8s-node-2    <none>           <none>
redis-slave-sts-0                                     1/1     Running   0          4d6h   10.233.64.137   sunstreaker-k8s-node-3    <none>           <none>
redis-slave-sts-1                                     1/1     Running   0          4d6h   10.233.65.119   sunstreaker-k8s-node-5    <none>           <none>
zookeper-sts-0                                        1/1     Running   0          4d6h   10.233.79.122   sunstreaker-k8s-node-4    <none>           <none>
[perf-user@sunstreaker-bastion-1 ~]$
```

2. Obtain the log information for the pods, run the command:

   ```
   kubectl logs <podName> -n <nameSpace>
   ```

Sample commands:

- `kubectl logs ocn-nwdaf-subscription-84f8b74cc7-d7lk9 -n performance-ns`

- `kubectl logs ocn-nwdaf-data-collection-57b948989c-xs7dq -n performance-ns`
- `kubectl logs ocn-nwdaf-gateway-584577d8b7-f2xvd -n performance-ns`
- `kubectl logs ocn-amf-simulator-584ccb8fd4-pcdn6 -n performance-ns`

5
OCNWDAF Alerts

This chapter includes information about the following alerts:

- Application Level Alerts
- System Level Alerts

5.1 Application Level Alerts

This section lists the application level alerts.

OCN_NWDAF_ANALYTICS_NOT_RUNNING

Table 5-1 OCN_NWDAF_ANALYTICS_NOT_RUNNING

Field	Details
Description	The microservice is not available or not reachable.
Cause	Microservice ocn-nwdaf-analytics is down.

OCN_NWDAF_COMMUNICATION_NOT_RUNNING

Table 5-2 OCN_NWDAF_COMMUNICATION_NOT_RUNNING

Field	Details
Description	The microservice is not available or not reachable.
Cause	Microservice ocn-nwdaf-communication is down.

OCN_NWDAF_CONFIGURATION_SERVICE_NOT_RUNNING

Table 5-3 OCN_NWDAF_CONFIGURATION_SERVICE_NOT_RUNNING

Field	Details
Description	The microservice is not available or not reachable.
Cause	Microservice ocn-nwdaf-configuration-service is down.

OCN_NWDAF_DATA_COLLECTION_NOT_RUNNING

Table 5-4 OCN_NWDAF_DATA_COLLECTION_NOT_RUNNING

Field	Details
Description	The microservice is not available or not reachable.
Cause	Microservice ocn-nwdaf-data-collection is down.

OCN_NWDAF_GATEWAY_NOT_RUNNING

Table 5-5 OCN_NWDAF_GATEWAY_NOT_RUNNING

Field	Details
Description	The microservice is not available or not reachable.
Cause	Microservice ocn-nwdaf-gateway is down.

OCN_NWDAF_MTLF_NOT_RUNNING

Table 5-6 OCN_NWDAF_MTLF_NOT_RUNNING

Field	Details
Description	The microservice is not available or not reachable.
Cause	Microservice ocn-nwdaf-mtlf is down.

OCN_NWDAF_SUBSCRIPTION_NOT_RUNNING

Table 5-7 OCN_NWDAF_SUBSCRIPTION_NOT_RUNNING

Field	Details
Description	The microservice is not available or not reachable.
Cause	Microservice ocn-nwdaf-subscription is down.

HIGH_ABNORMAL_BEHAVIOUR_REQUEST_RATE

Table 5-8 HIGH_ABNORMAL_BEHAVIOUR_REQUEST_RATE

Field	Details
Description	The number of requests received per second is high.
Cause	Traffic is high, above 1000 requests per second.
URI Endpoint	`nnwdaf-analyticsinfo/v1/analytics?event-id=ABNORMAL_BEHAVIOUR`
Affected Functions	ABNORMAL_BEHAVIOUR

HIGH_UE_MOBILITY_REQUEST_RATE

Table 5-9 HIGH_UE_MOBILITY_REQUEST_RATE

Field	Details
Description	The number of requests received per second is high.

Table 5-9 (Cont.) HIGH_UE_MOBILITY_REQUEST_RATE

Field	Details
Cause	Traffic is high, above 1000 requests per second.
URI Endpoint	`nnwdaf-analyticsinfo/v1/analytics?event-id=UE_MOBILITY`
Affected Functions	UE_MOBILITY

HIGH_EVENT_SUBSCRIPTION_REQUEST_RATE

Table 5-10 HIGH_EVENT_SUBSCRIPTION_REQUEST_RATE

Field	Details
Description	The number of requests received per second is high.
Cause	Traffic is high, above 1000 requests per second.
URI Endpoint	`nnwdaf-eventssubscription/v1/subscriptions`
Affected Functions	UE_MOBILITY, SLICE_LOAD_LEVEL, ABNORMAL_BEHAVIOUR

HIGH_ABNORMAL_BEHAVIOUR_REQUEST_FAILURE_RATE

Table 5-11 HIGH_ABNORMAL_BEHAVIOUR_REQUEST_FAILURE_RATE

Field	Details
Description	The number of requests failing per second is high.
Cause	The request failing rate is more than the 70%.
URI Endpoint	`nnwdaf-analyticsinfo/v1/analytics?event-id=ABNORMAL_BEHAVIOUR`
Affected Functions	ABNORMAL_BEHAVIOUR

HIGH_UE_MOBILITY_REQUEST_FAILURE_RATE

Table 5-12 HIGH_ABNORMAL_BEHAVIOUR_REQUEST_FAILURE_RATE

Field	Details
Description	The number of requests failing per second is high.
Cause	The request failing rate is more than the 70%.
URI Endpoint	`nnwdaf-analyticsinfo/v1/analytics?event-id=UE_MOBILITY`
Affected Functions	UE_MOBILITY

HIGH_EVENT_SUBSCRIPTION_REQUEST_FAILURE_RATE

Table 5-13 HIGH_EVENT_SUBSCRIPTION_REQUEST_FAILURE_RATE

Field	Details
Description	The number of requests failing per second is high.
Cause	The request failing rate is more than the 70%.
URI Endpoint	`nnwdaf-eventssubscription/v1/subscriptions`
Affected Functions	UE_MOBILITY, SLICE_LOAD_LEVEL, ABNORMAL_BEHAVIOUR

5.2 System Level Alerts

This section lists the system level alerts.

OCN_NWDAF_ANALYTICS_HIGH_CPU_LOAD

Table 5-14 OCN_NWDAF_ANALYTICS_HIGH_CPU_LOAD

Field	Details
Description	CPU load is high at the pod where the microservice is running.
Affected Functions	All
Cause	CPU load is more than 80% of the allocated resources.

OCN_NWDAF_COMMUNICATION_HIGH_CPU_LOAD

Table 5-15 OCN_NWDAF_COMMUNICATION_HIGH_CPU_LOAD

Field	Details
Description	CPU load is high at the pod where the microservice is running.
Affected Functions	All
Cause	CPU load is more than 80% of the allocated resources.

OCN_NWDAF_CONFIGURATION_SERVICE_HIGH_CPU_LOAD

Table 5-16 OCN_NWDAF_CONFIGURATION_SERVICE_HIGH_CPU_LOAD

Field	Details
Description	CPU load is high at the pod where the microservice is running.
Affected Functions	All

Table 5-16 (Cont.)
OCN_NWDAF_CONFIGURATION_SERVICE_HIGH_CPU_LOAD

Field	Details
Cause	CPU load is more than 80% of the allocated resources.

OCN_NWDAF_DATA_COLLECTION_HIGH_CPU_LOAD

Table 5-17 OCN_NWDAF_DATA_COLLECTION_HIGH_CPU_LOAD

Field	Details
Description	CPU load is high at the pod where the microservice is running.
Affected Functions	All
Cause	CPU load is more than 80% of the allocated resources.

OCN_NWDAF_GATEWAY_HIGH_CPU_LOAD

Table 5-18 OCN_NWDAF_GATEWAY_HIGH_CPU_LOAD

Field	Details
Description	CPU load is high at the pod where the microservice is running.
Affected Functions	All
Cause	CPU load is more than 80% of the allocated resources.

OCN_NWDAF_MTLF_HIGH_CPU_LOAD

Table 5-19 OCN_NWDAF_MTLF_HIGH_CPU_LOAD

Field	Details
Description	CPU load is high at the pod where the microservice is running.
Affected Functions	All
Cause	CPU load is more than 80% of the allocated resources.

OCN_NWDAF_SUBSCRIPTION_HIGH_CPU_LOAD

Table 5-20 OCN_NWDAF_SUBSCRIPTION_HIGH_CPU_LOAD

Field	Details
Description	CPU load is high at the pod where the microservice is running.
Affected Functions	All

Table 5-20 (Cont.) OCN_NWDAF_SUBSCRIPTION_HIGH_CPU_LOAD

Field	Details
Cause	CPU load is more than 80% of the allocated resources.

OCN_NWDAF_ANALYTICS_HIGH_JVM_HEAP_MEMORY_USAGE

Table 5-21 OCN_NWDAF_ANALYTICS_HIGH_JVM_HEAP_MEMORY_USAGE

Field	Details
Description	The average of the memory heap usage is high.
Affected Functions	All
Cause	The heap memory usage is more than the 80%.

OCN_NWDAF_COMMUNICATION_HIGH_JVM_HEAP_MEMORY_USAGE

Table 5-22 OCN_NWDAF_COMMUNICATION_HIGH_JVM_HEAP_MEMORY_USAGE

Field	Details
Description	The average of the memory heap usage is high.
Affected Functions	All
Cause	The heap memory usage is more than the 80%.

OCN_NWDAF_CONFIGURATION_SERVICE_HIGH_JVM_HEAP_MEMORY_USAGE

Table 5-23 OCN_NWDAF_CONFIGURATION_SERVICE_HIGH_JVM_HEAP_MEMORY_USAGE

Field	Details
Description	The average of the memory heap usage is high.
Affected Functions	All
Cause	The heap memory usage is more than the 80%.

OCN_NWDAF_DATA_COLLECTION_HIGH_JVM_HEAP_MEMORY_USAGE

Table 5-24 OCN_NWDAF_DATA_COLLECTION_HIGH_JVM_HEAP_MEMORY_USAGE

Field	Details
Description	The average of the memory heap usage is high.
Affected Functions	All
Cause	The heap memory usage is more than the 80%.

OCN_NWDAF_GATEWAY_HIGH_JVM_HEAP_MEMORY_USAGE

Table 5-25 OCN_NWDAF_GATEWAY_HIGH_JVM_HEAP_MEMORY_USAGE

Field	Details
Description	The average of the memory heap usage is high.
Affected Functions	All
Cause	The heap memory usage is more than the 80%.

OCN_NWDAF_MTLF_HIGH_JVM_HEAP_MEMORY_USAGE

Table 5-26 OCN_NWDAF_MTLF_HIGH_JVM_HEAP_MEMORY_USAGE

Field	Details
Description	The average of the memory heap usage is high.
Affected Functions	All
Cause	The heap memory usage is more than the 80%.

OCN_NWDAF_SUBSCRIPTION_HIGH_JVM_HEAP_MEMORY_USAGE

Table 5-27 OCN_NWDAF_SUBSCRIPTION_HIGH_JVM_HEAP_MEMORY_USAGE

Field	Details
Description	The average of the memory heap usage is high.
Affected Functions	All
Cause	The heap memory usage is more than the 80%.