Oracle® Communications

InterWorking and Mediation Function (IWF) Cloud Native Installation Guide

Release 1.5
F33289-01
July 2020

ORACLE

Oracle Communications InterWorking and Mediation Function (IWF) Cloud Native Installation Guide, Release 1.5

F33289-01

Contents

A IWF Yaml Files

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

New or Updated Features in Release 1.5:

This section introduces the documentation updates for Release 1.5 in IWF Installation Guide.

- Improving observability: Updated Metrics, KPIs, Alerts, logging and SNMP MIBs
- API Gateway Integration: Added Integrated Ingress/ Egress gateway parameters

List of Tables

1
IWF Installation Overview

This sections provides overview information of IWF.

The Oracle Communications 5G InterWorking and Mediation Function (IWF) enables 5G Core NFs to communicate with Evolved Packet Core (EPC) network elements. IWF is a Cloud Native solution based on microservices architecture that is deployed as an independent network function in the 5G network or as an independent microservice within the 5GC NF, as a part of Oracle 5GC NFs like NRF, SEPP, SCP, and so on.

IWF includes the following features:

- Protocol Translation:
  - IWF allows 5GC NF to interwork with the EPC network elements or vice versa.
  - IWF supports protocol conversion capabilities from Diameter to HTTP/2 and vice versa.
- Message Mediation:
  - This feature allows API transformation to resolve inter-NF inter operational issues.
  - Allows users to create policy rules to execute mediation transformation.

References

- CNE Install Guide
- IWF User's Guide

Acronyms and Terminologies

The following table provides information about the acronyms and terminologies used in the document.

Table 1-1 Acronyms and Terminologies

Field	Description
5GC	5G Core Network
API	Application Program Interface
CNE	Cloud Native Environment
DWR	Device Watchdog Request
EPC	Evolved Packet Core
IWF	InterWorking and Mediation Function
NEF	Network Exposure Function
NF	Network Function

Table 1-1 (Cont.) Acronyms and Terminologies

Field	Description
NRF	Network Repository Function
OSDC	Oracle Software Delivery Cloud
SCP	Service Communication Proxy
SEPP	Security Edge Protection Proxy
UDP	User Defined Protocol

2
IWF Prerequisites

This section includes information about the necessary prerequisites for IWF deployment.

Following are the prerequisites to install and configure IWF:

- Kubernetes Cluster must be available with Kube DNS configured to talk to operator's DNS server.
- Service FQDN of IWF must be discoverable from outside of cluster (i.e. publicly exposed if ingress messages to IWF can come from outside of K8S).
- The user must have own repository for storing the IWF images and repository must be accessible from the Kubernetes cluster.
- Primary/Management node must have installed with jq tool, later which will be used by config map content parsing tools

IWF Software

The IWF software includes:

- IWF Helm chart
- IWF docker images

The following software must be installed:

Software	Version
Kubernetes	v 1.15.3
HELM	v 2.14.3

Additional software that needs to be deployed as per the requirement of the services:

Software	Chart Version	Notes
elasticsearch	1.21.1	Needed for Logging Area
elastic-curator	1.2.1	Needed for Logging Area
elastic-exporter	1.1.2	Needed for Logging Area
logs	2.0.7	Needed for Logging Area
kibana	1.5.2	Needed for Logging Area
grafana	2.2.0	Needed for Metrics Area
prometheus	8.8.0	Needed for Metrics Area
prometheus-node-exporter	1.3.0	Needed for Metrics Area
metallb	0.8.4	Needed for External IP
metrics-server	2.4.0	Needed for Metric Server
tracer	0.8.3	Needed for Tracing Area

> **Note:**
>
> If any of the software specified in the above table is not installed in CNE, install the software. If OCCNE is the platform, then refer *Cloud Native Environment Installation Guide*.

Network access

The Kubernetes cluster hosts must have network access to:

- Local docker image repository where the IWF images are available.
- Local helm repository where the IWF helm charts are available.

> **Note:**
>
> All the kubectl and helm related commands that are used in this document must be executed on a system depending on the infrastructure of the deployment. It could be a client machine, VM, server, local desktop and so on.

Client machine requirement

There are some requirements for the client machine where the deployment commands need to be executed:

- It must have network access to the helm repository and docker image repository.
- Helm repository must be configured on the client.
- It should have network access to the Kubernetes cluster.
- It should have necessary environment settings to run the `kubectl` commands. The environment should have privileges to create namespace in the Kubernetes cluster.
- It should have helm client installed. The environment should be configured so that the `helm install` command deploys the software in the Kubernetes cluster.
- Master/Management node must have the `jq` tool installed to be used by configuration map content parsing tools.
- Operator must create MySQL NDB database cluster to store the configuration and run time data.

3
IWF Installation Sequence

This section informs about the installation sequence for IWF installation.

IWF Installation Sequence

1. **Installation Preparation**
2. **Configure `custom_values.yaml` file.**

   This includes configuring the following based on the deployment:

   a. Repository path.

   b. IWF details.
3. **Deploy IWF.**

   IWF can be deployed in the following ways:

   a. With HELM repository

   b. With Local repository
4. **Verify IWF deployment**

IWF Images

Table 3-1 IWF Images

Micro service	Image
ociwf-iwf-mediation	ocmed-iwfmediation:1.5.0
ociwf-iwf-diameterproxy	ociwf-iwfdiamproxy:1.5.0
ociwf-iwf-d2h	ociwf-iwfd2h:1.5.0
ociwf-iwf-h2d	ociwf-iwfh2d:1.5.0
ociwf-nf-mediation	ocmed-nfmediation:1.5.0
ociwf-pcf-diam-gateway	diam-gateway:1.5.0
ociwf-iwf-pcfdiscovery	ociwf-iwfpcfdiscovery:1.5.0
ociwf-iwf-mediation-test	ocmed-iwfmediation:1.5.0
ociwf-nf-mediation-test	ocmed-nfmediation:1.5.0
ociwf-iwf-iwfconfigmgr	ociwf-iwfconfigmgr:1.5.0
ociwf-appinfo	app_info:1.5.1
ociwf-performance	perf_info:1.5.0
ociwf-nrf-client-nfdiscovery	nrf-client:1.2.2
ociwf-ocpm-config	config_server:1.5.0
readiness-detector	nrf-client/readiness-detector:latest
ingress-gateway	ocingress_gateway:1.7.4
egress-gateway	ocegress_gateway:1.7.4

4
IWF Installation Preparation

This section includes information about the preparation required before IWF installation.

For more information about configuring docker image and registry, refer to OCCNE Docker Image Registry Configuration in *OCCNE Installation Guide.*

IWF Installation Preparation

1. **Download the OCIWF package:**

   Customers are required to download the OCIWF package from Oracle Software Delivery Cloud (OSDC). Package is named as follows:

   ```
   <nfname>-pkg-<marketing-release-number>.tgz
   ```

   ```
   Example:ociwf-pkg-1.5.0.0.0.tgz
   ```

2. **Untar the OCIWF Package:**

   Untar the OCIWF package into a specific repository:

   ```
   tar -xvf <<nfname>-pkg-<marketing-release-number>>
   ```

   The package file consists of following:

   a. OCIWF Docker Images tar
      `ociwf-images-1.5.0.tar`
   b. Helm File
      `ociwf-1.5.0.tgz`
   c. Readme txt file
      `Readme.txt` (Contains cksum and md5sum of tarballs)

3. **Check the checksums:**
   Check the checksums of tarballs mentioned in `Readme.txt`. Refer to the `Readme.txt` file for commands and checksum details.

4. **Load the tarball to system:**

   Execute the following command to push the Docker images to docker registry:

   ```
   docker load --input ociwf-images-1.5.0.tar
   ```

5. **Check if all the images are loaded:**

   Execute the following command to check:

   ```
   docker images
   ```

Refer table **IWF Images** in section IWF Installation Sequence for the list of images.

6. **Push docker images to docker registry:**

   Execute the following commands to push the docker images to docker registry:

   ```
   docker tag <image-name>:<image-tag> <docker-repo>/<image-name>:<image-tag>
   ```

   ```
   docker push <docker-repo>/<image-name>:<image-tag>
   ```

7. **Untar Helm Files:**

   Untar the helm files:

   ```
   tar -xvzf ociwf-1.5.0.tgz
   ```

8. **Download the InterWorking and Mediation Function (IWF) Custom Template ZIP file:**

   Download the **InterWorking and Mediation Function (IWF) Custom Template** ZIP file from OHC:

   - Go to the Oracle Help Center (OHC) Web site: https://docs.oracle.com
   - Navigate to Industries >Communications >Cloud Native Core >Release 2.2.1
   - Click the **InterWorking and Mediaiton Function (IWF) Custom Template** link to download the zip file.
   - Unzip the template to get `ociwf-custom-values-1.5.0.yaml` file.
   - Customize the `ociwf-custom-values-1.5.0.yaml` file.
   - Save the updated `ociwf-custom-values-1.5.0.yaml` file in the helm chart directory.

5
IWF Installation

This section includes information about the OCIWF installation procedures.

IWF Deployment Procedure

The following procedure guides you through installation of OCIWF on CNE:

OCIWF Deployment

1. **Create Database User/Group:**

   Create User with permission to access the tables on all the SQL nodes present in the NDB cluster, by executing commands:

   Note:

   - The OCIWF uses a MySQL database to store the configuration and run time data.
   - The OCIWF deployment using MySQL NDB cluster requires the database administrator to create user in MYSQL DB and to provide the user with necessary permissions to access the tables in the NDB cluster.

   a. Login to the server where the ssh keys are stored and SQL nodes are accessible.

   b. Connect to the SQL nodes.
   `ssh <USERNAME>@<HOSTNAME>`

   c. Login to the MYSQL as a root user:
   `/usr/local/mysql/bin/mysql -h 127.0.0.1 -u root -p <password>`

   d. Create MYSQL user:

   ```
   CREATE USER '<USERNAME>'@'%' IDENTIFIED BY '<PASSWORD>';
   DROP DATABASE if exists iwfdb;
   CREATE DATABASE iwfdb CHARACTER SET utf8;
   GRANT SELECT, INSERT, CREATE, ALTER, DROP, LOCK TABLES,
   CREATE TEMPORARY TABLES, DELETE, UPDATE, EXECUTE ON iwfdb.* TO
   '<USERNAME>'@'%';
   ```

   e. Execute the following commands on one of the NDB SQL node:

      i. Log into the MYSQL user created in the previous step:
      `/usr/local/mysql/bin/mysql -h 127.0.0.1 -u <USERNAME> -p <PASSWORD>`

      ii. Create MYSQL table:

      ```
      USE iwfdb;
      CREATE TABLE IF NOT EXISTS session_correlation (
       SESSION_ID varchar(255) NOT NULL,
       RESOURCE_ID varchar(255) NOT NULL UNIQUE,
      ```

```
    PEER_IDENTITY varchar(255) NOT NULL,
    PEER_REALM varchar(255) NOT NULL,
    REQUEST_COUNT int(11),
    PRIMARY KEY (SESSION_ID)
   ) ENGINE=NDBCLUSTER DEFAULT CHARSET=utf8;
```

Note: The <username> and <password> is created by the Database Administrator.

f. Exit from database and logout from SQL node.

2. **Customize `ociwf-custom-values.yaml` file:**

   Customize `ociwf-custom-values.yaml` file as per the deployment requirement:

   Update service ports accordingly.

   For more information, see IWF Installation Preparation.

   To configure the parameters, see section IWF Configuration

   or,
   The `ociwf-custom-values-1.5.0.yaml` template can be downloaded from OHC.

   Download the InterWorking and Mediation Function (IWF) Custom Template ZIP file and Unzip to get `ociwf-custom-values-1.5.0.yaml` file.

   Refer Appendix for Sample IWF yaml file.

3. **Perform the Diameter configuration:**

   Configure diameter peer(s) in the following file:
   `ociwf/charts/pcf/templates/configmap-pcf-diam-gateway-service-diameter.yaml`

   Refer to **IWF User guide** for diameter peer configuration details.

4. **Update the BSF (Binding Support Function) Configuration:**

   Update the BSF details in the pcf Discovery section in the `ociwf-custom-values-1.5.0.yaml`

   - **BSF (Binding Support Function)**
     - Configuration bsfSvc: FQDN or IP of BSF service
     - bsfPort: Node Port of BSF service
   - **NRF Configuration**
     - requesterNfType: e.g. CUSTOM_IWF
     - targetNfType: e.g. BSF
   - **NRF Client configuration**
     - update primaryNrfApiRoot with fqdn of the deployed nrf's ingress gateway
     - update nrfClientType in profile (it must match with requesterNfType value provided in pcfDiscovery)

5. **Deploy IWF**

   a. Deploy IWF from Helm repository:
   To deploy IWF from Helm repository, execute:

   ```
   helm install ociwf/ -f <ociwf-custom-values.yaml> --name <helm-release> --namespace <k8s namespace> --version <ociwf version>
   ```

Example:

```
helm install ociwf-helm-repo/ociwf -f ociwf-custom-values.yaml --
name ociwf --namespace iwfsvc --version <ociwf version>
```

b. Deploy IWF from local repository:

To deploy IWF from local repository, execute:
`helm install ociwf -f <ociwf-custom-values.yaml> --name <helm-release> --namespace <k8s namespace>`

Example:

```
helm install ociwf -f ociwf-custom-values.yaml --name ociwf --
namespace iwfsvc
```

6. **Check status of the services:**

Execute the following command:
`kubectl get services -n <namespace>`

Example:

```
kubectl get services -n iwfsvc
```

```
NAME                              TYPE        CLUSTER-IP  EXTERNAL-IP
PORT(S)                          AGE
ociwf-egress-gateway             ClusterIP    10.111.86.188  <none>
8080/TCP                         2m49s
ociwf-egress-gateway-hazelcast ClusterIP   None           <none>
5701/TCP                         2m49s
ociwf-ingress-gateway            LoadBalancer 10.97.224.26   <pending>
80:30075/TCP                     2m49s
ociwf-iwf-configmgr              LoadBalancer 10.102.127.159 <pending>
8080:30066/TCP                   2m49s
ociwf-iwf-d2h                    ClusterIP    10.105.189.19
<none>     8080/TCP                        2m49s
ociwf-iwf-diameterproxy          ClusterIP    10.98.135.5
<none>     8080/TCP                        2m49s
ociwf-iwf-h2d                    ClusterIP    10.111.72.93
<none>     8080/TCP                        2m49s
ociwf-iwf-mediation              LoadBalancer 10.110.149.7
<pending>  9090:30079/TCP,9091:30080/TCP2m48s
ociwf-iwf-mediation-test         ClusterIP    10.102.161.69
<none>      9090/TCP                       2m49s
ociwf-iwf-pcfdiscovery           ClusterIP    10.105.167.147
<none>      8080/TCP                        2m48s
ociwf-nf-mediation               LoadBalancer 10.107.119.17
<pending>   9090:30081/TCP,9091:30082/TCP2m48s
ociwf-nf-mediation-test          ClusterIP    10.104.203.244
<none>      9090/TCP                        2m48s
ociwf-ocpm-config                ClusterIP    10.98.223.36
<none>      5807/TCP,9000/TCP               2m48s
ociwf-pcf-diam-gateway           ClusterIP    None
<none>      8080/TCP,3868/TCP               2m49s
ociwf-pcf-diam-gateway-serviceNodePort     10.101.171.175
<none>      8080:30453/TCP,3868:30090/TCP   2m49s
```

Note: If `metallb` is used, `EXTERNAL-IP` is assigned to `ociwf-endpoint`.

7. **Check status of the pods:**

   Execute the following command:
   `kubectl get pods -n <ociwf_namespace>`

   Status column of all the pods should be 'Running'.

   Ready column of all the pods must be n/n, where n is number of containers in the pod.

   Example:

   ```
   kubectl get pods -n iwfsvc
   ```

   ```
   NAME                                      READY STATUS RESTARTS AGE
   ociwf-egress-gateway-5d86d7755b-8c4rx     1/1  Running  0  13s
   ociwf-ingress-gateway-6d5bdcd859-mn2pz    1/1  Running  0  13s
   ociwf-iwf-configmgr-65957546d5-jfwwr      1/1  Running  0  13s
   ociwf-iwf-d2h-d6ffd8788-qk52j             1/1  Running  0  13s
   ociwf-iwf-diameterproxy-56479d8c7-szcwh   1/1  Running  0  13s
   ociwf-iwf-h2d-6cfff7754d-ppmsk            1/1  Running  0  13s
   ociwf-iwf-mediation-66fbf5c98f-lzn2j      1/1  Running  0  13s
   ociwf-iwf-mediation-test-7c5dc59ff5-hsd4p 1/1  Running  0  13s
   ociwf-iwf-pcfdiscovery-67966f7b6b-4rvf4   1/1  Running  0  13s
   ociwf-nf-mediation-8554fcd55f-wnncw       1/1  Running  0  13s
   ociwf-nf-mediation-test-5cd6c489fd-86gdh  1/1  Running  0  13s
   ociwf-pcf-diam-gateway-0                  1/1  Running  0  13s
   ```

6
IWF Configuration

This section includes configuration options supported for IWF.

For detailed information about configuring parameters, see IWF Configurable Parameters.

Download the InterWorking and Mediation Function (IWF) Custom Template ZIP file from OHC and Unzip the template to get `ociwf-custom-values-1.5.0.yaml` file.

Mediation Test Mode configuration

IWF Mediation can be configured to send request and response to IWF Mediation Test Service by setting `test-mode-enable` to `True` in environment variable in the IWF Mediation deployment chart.

MYSQL Configuration

The MYSQL allows the operator to configure the database and store the association between the N5 and Rx session.

- Configurable options supported through custom values file `ociwf-custom-values-1.5.0.yaml`.
  1. Using CNE Mysql cluster
     a. Edit `iwf-mysql:enabled`: false (Disables the mysql pod)
     b. Edit `iwf-diameterproxy`:
        Enter the IP of the primary and secondary mysql nodes in the mysql cluster deployed in CNE.

        ```
        dpDBService1: <db connectivity service name>
        dpDBService2: <db connectivity service name>
        ```

        > **Note:**
        > Along with IP, the DB cluster credentials should be configured.

Updating Mediation Rule in the ConfigMap

Reloading the IWF-Mediation ConfigMap, if in case any updates were made in the Rules.

The tool `ociwf-rule-download_tool.sh` can be used to download the rule configmap in a folder (folder name will be configmap name). It needs namespace as well as required configmap name. These rules then can be changed accordingly.

The tool `ociwf-rule-upload_tool.sh` can be used to upload the rule config map from the existing config map folder. It needs namespace as well as required configmap name to be uploaded.

- If rules were changed on iwf active mediation, then use `ociwf-iwf-mediation-config-active` as the name of configmap.
- If rules were changed on iwf test mediation then use `ociwf-iwf-mediation-config-test` as the name of the configmap.

Reloading the NF-Mediation ConfigMap, if in case any updates were made in the Rules.

- The tool `ociwf-rule-download_tool.sh` can be used to download the rule configmap in a folder (folder name will be configmap name). It needs namespace as well as required configmap name. These rules then can be changed accordingly.
- The tool `ociwf-rule-upload_tool.sh` can be used to upload the rule config map from the existing config map folder. It needs namespace as well as required configmap name to be uploaded
- If rules were changed on nf active mediation, then execute `ociwf-nf-mediation-config-active` as the name of configmap
- If the rules were changed on nf test mediation, then execute: `ociwf-nf-mediation-config-test` as the name of the configmap.

> **Note:**
>
> The user can varify the status through container logs, Prometheus metrics or graffana dashboards.

IWF-Mediation Rule Configuration for PT

Add below rules to the mediation rules:

> **Note:**
>
> In the below rules, replace `PCF_loadBalancerIP_and_Port` and `IWF_loadBalancerIP_and_Port` with appropriate values.

```
rule "pt_d2h_to_nf_rule"
salience 1
when
    req : Request(headers.has("pt_dest_uri"))
then

req.setUri(req.headers.get("pt_dest_uri").replace("pcf.com","10.75.203.7
4:1000/simulation"))
    req.headers.del("pt_dest_uri")
end

rule "pt_rar_to_pcf_rule"
salience 1
when
```

```
  req : Request(req.getUri().toString() matches ".*(npcf-
policyauthorization)*(v1)*(notification)*(notify).*")
then
 req.getHttpMessageFactImpl().forwardPath = IWFConsts.FORWARD_TO_H2D
 req.headers.add("diameterApplicationId","16777236")
 req.headers.add("diameterCommandCode","258")
 req.headers.add("original-req-uri",req.getUri())
end

rule "pt_aar_to_pcf_rule"
salience 1
when
  req : Request(req.body.has("$.ascReqData.notifUri"))
then

req.body.add("$.ascReqData.notifUri",req.body.get("$.ascReqData.notifUri
").toString().replace("iwf.com","10.75.203.74:30079"))

req.body.add("$.ascReqData.evSubsc.notifUri",req.body.get("$.ascReqData.
evSubsc.notifUri").toString().replace("iwf.com","10.75.203.74:30079"))
end

rule "pt_asr_to_pcf_rule"
salience 1
when
  req : Request(getUri().toString() matches ".*(npcf-
policyauthorization)*(v1)*(notification)*(terminate).*")
then
  req.getHttpMessageFactImpl().forwardPath=IWFConsts.FORWARD_TO_H2D
  req.headers.add("diameterApplicationId","16777236")
  req.headers.add("diameterCommandCode","274")
  req.headers.add("original-req-uri",req.getUri())
end


rule "pt_ccri_to_h2d_rule"
salience 1
when
req : Request(req.getUri() matches ".*(npcf-smpolicycontrol/v1/sm-
policies)(/$|$)")
then
req.getHttpMessageFactImpl().forwardPath=IWFConsts.FORWARD_TO_H2D
req.headers.put("diameterApplicationId","16777238")
req.headers.put("diameterCommandCode","272")
req.headers.put("requestType","CREATE")
end

rule "pt_ccru_to_h2d_rule"
salience 1
when
req : Request(req.getUri() == ".*(npcf-smpolicycontrol/v1/sm-policies/)
(.*)(/update)(/$|$)")
then
req.getHttpMessageFactImpl().forwardPath=IWFConsts.FORWARD_TO_H2D
req.headers.put("diameterApplicationId","16777238")
```

```
req.headers.put("diameterCommandCode","272")
req.headers.put("requestType","UPDATE")
req.headers.put("original-req-uri",req.getUri())
end

rule "pt_ccrt_to_h2d_rule"
salience 1
when
req : Request(req.getUri() matches ".*(npcf-smpolicycontrol/v1/sm-
policies/)(.*)(/delete)(/$|$)")
then
req.getHttpMessageFactImpl().forwardPath=IWFConsts.FORWARD_TO_H2D
req.headers.put("diameterApplicationId","16777238")
req.headers.put("diameterCommandCode","272")
req.headers.put("requestType","DELETE")
req.headers.put("original-req-uri",req.getUri())
end
```

NF-Mediation Rule Configuration

Add below rules to the mediation rules:

```
function Map<Object, Object> addObject() {
    return new HashMap<Object, Object>();
}

function ArrayList<Object> addArray() {
    return new  ArrayList<Object>();
}

function Map<String,Object> ipEndPoints(String ipv4Address, String
ipv6Address, String ipv6Prefix){
        Map< String,Object> ipEndPointObj = new HashMap<
String,Object>();
        ipEndPointObj.put("ipv4Address", ipv4Address);
        ipEndPointObj.put("ipv6Address", ipv6Address);
        ipEndPointObj.put("ipv6Prefix",ipv6Prefix );
        return ipEndPointObj;
}

rule "New Rule1"
    agenda-group "scp"
when
    req : Request(body.get("$.apiPrefix")=="/mediation")
then
    req.headers.put("x-dest-
path",req.body.get("$.apiPrefix").toString())
end

rule "New Rule2"
when
    req :
Request(body.has("$.defaultNotificationSubscriptions[*].callbackUri","pc
f.oracle.com/pcs/v1.0/nrf/notifycallback"))
then
```

```
req.body.add("$.ipEndPoints",ipEndPoints("10.75.243.193","2001:0db8:85a3
:0000:0000:8a2e:0370:7335","2001:0db8:85a3"))

end

rule "New Rule3"
when
    req : Request(headers.has("x-forwarded-NF","PCF") &&
body.has("$.fqdn","pcf.oracle.com"))
then
    req.headers.put("x-forwarded-NF","AMF")
    req.body.put("$","fqdn","amf.oracle.com")
end

rule "New Rule4"
when
    req : Request(body.get("$.serviceName")=="svc1")
then
    req.headers.del("x-service-name")
end

rule "New Rule5"
when
   req : Request(headers.get("x-number")  in (1,2,3,4,5 ))
then
   req.headers.put( "x-original-authority", "10.172.19.110:8080")
end
```

7

IWF Configurable Parameters

This section includes information about configurable parameters required during IWF installation.

The following tables describes the configuration parameters for each micro service that is configured during IWF deployment using `ociwf-custom.values.yaml` file:

pcf-gateway Microservice

Table 7-1 pcf-gateway Microservice

Parameter	Description	Default Value
global.dockerRegistry	Image repo	cgbudocker.us.oracle.com :5655
global.imageTag	Image tag	latest
pcf.deploymentOcpmPcfDiamGateway.envGatewayMode	Mode of gateway	bsf
pcf.deploymentOcpmPcfDiamGateway.image	Name of the image	diam-gateway
pcf.deploymentOcpmPcfDiamGateway.imageTag	Tag of the Image	1.5.0
pcf.hostIp	Host IP	slave1=10.196.46.13

iwf-mediation

Table 7-2 IWF Mediation Microservice

Parameter	Description	Default Value
image.name	Image name	ocmed-iwf-mediation
image.repository	Image repository name	reg-1:5000
image.tag	Tag of Image	1.5.0
service.active.ForwardToTest	Whether Trial rule test needs to be enabled or not	Disable
service.active.nodePortHttp	Http port to receive traffic	30079
service.active.nodePortHttps	Https port to receive traffic	30080

iwf-mediation-test Microservice

Table 7-3 iwf-mediation-test Microservice

Parameter	Description	Default Value
image.repository	Image repository name	reg-1:5000
Image name	Image name	ocmed-iwfmediation
image.tag	Tag of Image	1.5.0

nf-mediation

Table 7-4 NF Mediation Microservice

Parameter	Description	Default Value
image.name	Image name	ocmed-nf-mediation
image.repository	Image repository name	reg-1:5000
image.tag	Tag of Image	1.5.0
service.active.ForwardToTest	Whether Trial rule test needs to be enabled or not	Disable
service.active.nodePortHttp	Http port to receive traffic	30081
service.active.nodePortHttps	Https port to receive traffic	30082

nf-mediation-test Microservice

Table 7-5 nf-mediation-test Microservice

Parameter	Description	Default Value
image.repository	Image repository name	reg-1:5000
Image name	Image name	ocmed-nfmediation
image.tag	Tag of Image	1.5.0

iwf-d2h

Table 7-6 IWF D2H Microservice

Parameter	Description	Default Value
image.repository	Image repository name	reg-1:5000
image.name	Image name	ociwf-iwfd2h
image.tag	Tag of Image	1.5.0
opentracingHost	Kubernetes master node IP addres	127.0.0.1 (Customer must provide the correct IP address)
opentracingPort	UDP node port of Jaeger-Agent	0 (Customer must provide the correct port)

iwf-h2d

Table 7-7 IWF H2D Microservice

Parameter	Description	Default Value
image.repository	Image repository name	reg-1:5000
image.name	Image name	ociwf-iwfh2d
image.tag	Tag of Image	1.5.0
opentracingHost	Kubernetes master node IP address	127.0.0.1 (Customer must provide the correct IP address)
opentracingPort	UDP node port of Jaeger-Agent	0 (Customer must provide the correct port)

iwf-diameterproxy

Table 7-8 IWF Diameter Proxy Microservice

Parameter	Description	Default Value
image.repository	Image repository name	reg-1:5000
image.name	Image name	ociwf-iwfdiamproxy
image.tag	Tag of Image	1.5.0
DIAMETER_Realm	Diameter Realm of PT diameter node	Customer must provide the realm to be used
DIAMETER_Identity	FQDN of PT diameter node	Customer must provide the FQDN to be used
dpDBService1	MySQL cluster's node-1 IP address or MySQL K8s service name	iwf-pt-mysql-svc (customer must provide correct value)
dpDBService2	MySQL cluster's node-2IP addressor MySQL K8s service name	iwf-pt-mysql-svc (customer must provide correct value)
opentracingHost	Kubernetes master node IP address	127.0.0.1 (Customer must provide the correct IP address)
opentracingPort	UDP node port of Jaeger-Agent	0 (Customer must provide the correct port)
pcfDiscoveryMode	Flag which enables to switch modes(PDRA and D2H)	true
connectorMode	Mode of Diameter Connector	bsf

iwf-mysql

Table 7-9 IWF MYSQL Microservice

Parameter	Description	Default Value	Notes
enabled	Option to provision local K8s MySQL pod	false	Customer needs to fill it. When set to true the local mysql pod is brought up (Note: This is only for testing purpose, not for production. Production environment is expected to use MySQL cluster)
mysqlUser	MySQL User name	iwfusr	Customer needs to fill the user name to be used **Note**: This is only applicable when the above mentioned "enabled" option is set to true, else customer need not configure.
mysqlPassword	MySQL User password		Customer needs to fill the user password to be used (Note: This is only applicable when the above mentioned "enabled" option is set to true, else customer need not configure)

Table 7-9 (Cont.) IWF MYSQL Microservice

Parameter	Description	Default Value	Notes
initialization Files.iwf-db.sql	Mysql ddl commands to be run while deploying the Mysql pod	CREATE DATABASE IF NOT EXISTS iwfdb DEFAULT CHARACTER SET utf8 DEFAULT COLLATE utf8_general_ci;	Should Not be changed (Note: This is only applicable when the above mentioned "enabled" option is set to true, else customer need not configure)
initialization Files.permission.sql	Mysql permission to the user	GRANT ALL PRIVILEGES ON *.* TO 'iwfusr'@'%';	Customer needs to edit the "user name" in the command command, based on the value set to " mysqlUser" option. (Note: This is only applicable when the above mentioned "enabled" option is set to true, else customer need not configure)

iwf-nrfclient

Table 7-10 IWF NRF Client Microservice

Parameter	Description	Default Value
ociwf-appinfo	For checking the status of the NF's registered services	app_info:1.5.1
ociwf-performance	For monitoring and analysis of the services to probe performance data, and provide analysis output including load, capacity	perf_info:1.5.0
ociwf-nrf-client-nfdiscovery	For performing NfRegistration, NfSubscription and NfDiscovery	nrf-client:1.2.2
ociwf-ocpm-config		config_server:1.5.0
readiness-detector		nrf-client/readiness-detector:latest

iwf-pcfdiscovery

Table 7-11 iwf-pcfdiscovery Microservice

Parameter	Description	Default Value
image.repository	Image repository Name	reg-1:5000
image.name	Image Name	ociwf
image.tag	Tag or Image	1.5.0
opentracingHost	Kubernetes master node IP address	127.0.0.1 (Customer must provide the correct IP address)

Table 7-11 (Cont.) iwf-pcfdiscovery Microservice

Parameter	Description	Default Value
opentracingPort	UDP node port of Jaeger-Agent	0 (Customer must provide the correct port)
bsfSvc	Service or IP of the BSF	
bsfPort	Port of the BSF	8080

Diameter Peer configuration

Peer nodes are configured in gateway in `configmap-pcf-diam-gateway-service-diameter.yaml` file in location of `chart pcf/templates`

The sample is provided below:

```
apiVersion: v1
kind: ConfigMap
metadata:
 name: pcf-diam-gateway-config-peers
data:
  diameter-config-peers: |
    version: '0.3'
     kind: 'diameter-config'
    metadata:
      label: 'diameter-config-peers'
    setting:
      reconnectDelay: 3
      responseTimeout: 5
      connectionTimeOut: 3
      watchdogInterval: 6
      transport: 'TCP'
    # type: [af, dra]
    nodes:
      - name: 'P-CSCF'
        type: 'pcrf'
        responseOnly: true
        host: '10.75.215.205'
        port: 3880
        realm: 'ociwf.oracle.com'
        identity: 'pcrfsim.ociwf.oracle.com'
```

Parameters		Definitions
reconnectDelay		Time delay in seconds between successive peer connection establishment attempts
responseTimeout		Response timer value in seconds
connectionTimeOut		Connection timer value in seconds
watchdogInterval		Inactivity time in seconds after which DWR will be triggered
transport		Transport protocol type "TCP"
Nodes (list)	name	Name of the peer node

Parameters		Definitions
	responseOnly	Indicates the Diameter GW proxy client or server
	host	IP address of the peer node
	port	Port on which peer node listens for connections
	realm	Realm of the peer node
	identity	FQDN of the peer node

ingress-gw Microservice

Parameter	Description	Mandatory Parameter	Default value
image.repository	Image repository name	Yes	reg-1:5000
image.name	Image name	Yes	ocingress_gateway
image.tag	Tag of Name	Yes	1.7.4

Table 7-12 Ingress Gateway

Name	Description	Default Value	Mandatory	Notes
global.dockerRegistry	Name of the Docker registry which hosts Ingress docker images.	ocnrf-registry.us.oracle.com:5000	Yes	This is the registry which has docker images. Change this value if there is a need.
global.type	type of service	LoadBalancer	Yes	Possible values are :- ClusterIP, NodePort, LoadBalancer and ExternalName
global.serviceAccountName	Service Account name	''	No	
global.metalLbIpAllocationEnabled	Enable or disable IP Address allocation from Metallb Pool	true	No	
global.metalLbIpAllocationAnnotation	Address Pool Annotation for Metallb	metallb.universe.tf/address-pool: signaling	No	

Table 7-12 (Cont.) Ingress Gateway

Name	Description	Default Value	Mandatory	Notes
global.staticIpAddressEnabled	If Static load balancer IP needs to be set, then set staticIpAddressEnabled flag to true and provide value for staticIpAddress Else random IP will be assigned by the metalLB from its IP Pool	false	No	
global.staticIpAddress	StaticIp	10.75.212.60		
global.publicHttpSignalingPort	Http Signaling port	80	Yes	
global.publicHttpsSignallingPort	Https Signaling port	443	Yes	
global.staticNodePortEnabled	Node Port Enabled	true	No	
global.staticHttpNodePort	Http Node Port	30075	Yes	
global.staticHttpsNodePort	Https Node Port	30043	Yes	
global.configServerFullNameOverride	This parameter is for the usage of policy teams. Other teams can ignore this parameter.		No	
enableOutgoingHttps	Enabling it for outgoing https request	false	Yes	Change it to true for enabling https for outgoing requests.
enableIncomingHttp	Enabling it for incoming http request	false	Yes	
enableIncomingHttps	Enabling it for incoming https request	true	Yes	
enablehttp1	Enable it for http1.1	false	No	Change it to true to enable
dnsRefreshDelay	Dns Refresh Delay in milli-seconds	120000	No	
oauthValidatorEnabled	Oauth Validator Enabled	false	Yes	Change it to true to enable oauth
jaegerTracingEnabled	Enable jaeger tracing	false	No	Change it to true if needed.
openTracing.jaeger.udpSender.host	Jaeger Host	jaeger-agent.cne-infra	Yes (If jaegerTracingEnabled is true)	

Table 7-12 (Cont.) Ingress Gateway

Name	Description	Default Value	Mandatory	Notes
openTracing.jaeger.udpSender.port	Jaeger Port	6831	Yes (If jaegerTracingEnabled is true)	
openTracing.jaeger.probabilisticSampler		0.5	Yes (If jaegerTracingEnabled is true)	
nfType	NFType of service producer.	Value to be updated accordingly	Yes (When oauthValidatorEnabled)	
nfInstanceId:	NF InstanceId of service producer.	Value to be updated accordingly	Yes (When oauthValidatorEnabled)	
producerScope:	Comma-separate list of services hosted by service producer.	Value to be updated accordingly	Yes (When oauthValidatorEnabled)	
allowedClockSkewSeconds	set this value if clock on the parsing NF(producer) is not perfectly in sync with the clock on the NF(consumer) that created the JWT.	0	Yes (When oauthValidatorEnabled)	
nrfPublicKeyKubeSecret	Name of the secret which stores the public key(s) of NRF.	Value to be updated accordingly	Yes (When oauthValidatorEnabled)	
nrfPublicKeyKubeNamespace	Namespace of the NRF publicKey Secret	Value to be updated accordingly	Yes (When oauthValidatorEnabled)	
validationType	Values can be "strict" or "relaxed". "strict" means that incoming request without "Authorization" (Access Token) header will be rejected."relaxed" means that if incoming request contains "Authorization" header, it will be validated. If incoming request does not contain "Authorization" header, validation will be ignored.	Value to be updated accordingly	Yes (When oauthValidatorEnabled)	
producerPlmnMNC	MNC of service producer.	Value to be updated accordingly	No	
producerPlmnMCC	MCC of service producer.	Value to be updated accordingly	No	
cncc.enabled	CNCC Identity-Access-Management(IAM).	False	No	Change it to true if required.

Table 7-12 (Cont.) Ingress Gateway

Name	Description	Default Value	Mandatory	Notes
cncc.core.sessionTimeoutSeconds	Session Timeout Value in Seconds. Default: 1800, Minimum: 300, Maximum: 7200	1800	No	
cncclamEnabled	CNCC Identity-Access-Management (IAM)	false	No	Change it to true if required
ingressGwCertReloadEnabled		true	No	
rateLimiting.enabled	Ratelimiting feature enabled	false	No	
routeRateLimiting.enabled	Route based ratelimiting feature enabled	true	No	
globalIngressRateLimiting.enabled	Global rate limiting is enabled	true	No	
globalIngressRateLimiting.duration	Iterations of time duration (In seconds) for which bucketCapacity and refillRate are reset.	1 (in seconds)	yes (if globalIngressRateLimiting.enabled)	
globalIngressRateLimiting.burstCapacity	Holds maximum number of tokens in the bucket for the given duration.	1	yes (if globalIngressRateLimiting.enabled)	
globalIngressRateLimiting.refillRate	Number of tokens to be added to the bucket for the given duration	1	yes (if globalIngressRateLimiting.enabled)	
identityAccessMgt.uri	Identity access management uri		yes (if cncclamEnabled)	
identityAccessMgt.path	Identity access management path		yes (if cncclamEnabled)	
identityAccessMgt.realm	Identity access management realm		yes (if cncclamEnabled)	
identityAccessMgt.clientId	Identity access management client id		yes (if cncclamEnabled)	
iam.uri The section name is changed to iam	Identity access management uri		yes (if cncclamEnabled)	
iam.path	Identity access management path		yes (if cncclamEnabled)	
iam.realm	Identity access management realm		yes (if cncclamEnabled)	
iam.clientId	Identity access management client id		yes (if cncclamEnabled)	

Table 7-12 (Cont.) Ingress Gateway

Name	Description	Default Value	Mandatory	Notes
pingDelay	Delay between pings in seconds. When set to <=0,ping is disabled	60	Yes	PING frame can be scheduled at Ingress-gateway to maintain connection between Ingress-gateway and backend micro-services even if the connection is idle.
cfgServer.enabled	Config server switch. For the usage of Policy teams. For other NF's this has to be left false	false	No	
publicHttpSignalingPort	Http Signalling port	80	Yes	
publicHttpsSignallingPort	Https Signalling port	443	Yes	
ssl.privateKey.k8SecretName	Name of the privatekey secret	n/a	Yes (If enableIncomingHttp is true otherwise No)	
ssl.privateKey.k8NameSpace	Namespace of privatekey	n/a	Yes (If enableIncomingHttp is true otherwise No)	
ssl.privateKey.rsa.fileName	rsa private key file name	n/a	Yes (If enableIncomingHttp is true otherwise No)	
ssl.privateKey.ecdsa.fileName	ecdsa private key file name	n/a	Yes (If enableIncomingHttp is true otherwise No)	
ssl.certificate.k8SecretName	Name of the privatekey secret	n/a	Yes (If enableIncomingHttp is true otherwise No)	
ssl.certificate.k8NameSpace	Namespace of privatekey	n/a	Yes (If enableIncomingHttp is true otherwise No)	
ssl.certificate.rsa.fileName	rsa private key file name	n/a	Yes (If enableIncomingHttp is true otherwise No)	
ssl.certificate.ecdsa.fileName	ecdsa private key file name	n/a	Yes (If enableIncomingHttp is true otherwise No)	

Table 7-12 (Cont.) Ingress Gateway

Name	Description	Default Value	Mandatory	Notes
ssl.caBundle.k8SecretName	Name of the privatekey secret	n/a	Yes (If enableIncomingHttp is true otherwise No)	
ssl.caBundle.k8NameSpace	Namespace of privatekey	n/a	Yes (If enableIncomingHttp is true otherwise No)	
ssl.caBundle.rsa.fileName	rsa private key file name	n/a	Yes (If enableIncomingHttp is true otherwise No)	
ssl.keyStorePassword.k8SecretName	Name of the privatekey secret	n/a	Yes (If enableIncomingHttp is true otherwise No)	
ssl.keyStorePassword.k8NameSpace	Namespace of privatekey	n/a	Yes (If enableIncomingHttp is true otherwise No)	
ssl.keyStorePassword.fileName	File name that has password for keyStore	n/a	Yes (If enableIncomingHttp is true otherwise No)	
ssl.trustStorePassword.k8SecretName	Name of the privatekey secret	n/a	Yes (If enableIncomingHttp is true otherwise No)	
ssl.trustStorePassword.k8NameSpace	Namespace of privatekey	n/a	Yes (If enableIncomingHttp is true otherwise No)	
ssl.trustStorePassword.fileName	File name that has password for trustStore	n/a	Yes (If enableIncomingHttp is true otherwise No)	
publicHttpSignalingPort	Http Signalling port	80	Yes	
publicHttpsSignallingPort	Https Signalling port	443	Yes	
ssl.privateKey.k8SecretName	Name of the privatekey secret	n/a	Yes (If enableIncomingHttp is true otherwise No)	
ssl.privateKey.k8NameSpace	Namespace of privatekey	n/a	Yes (If enableIncomingHttp is true otherwise No)	

Table 7-12 (Cont.) Ingress Gateway

Name	Description	Default Value	Mandatory	Notes
ssl.privateKey.rsa.fileName	rsa private key file name	n/a	Yes (If enableIncomingHttp is true otherwise No)	
ssl.privateKey.ecdsa.fileName	ecdsa private key file name	n/a	Yes (If enableIncomingHttp is true otherwise No)	
ssl.certificate.k8SecretName	Name of the privatekey secret	n/a	Yes (If enableIncomingHttp is true otherwise No)	
ssl.certificate.k8NameSpace	Namespace of privatekey	n/a	Yes (If enableIncomingHttp is true otherwise No)	
ssl.certificate.rsa.fileName	rsa private key file name	n/a	Yes (If enableIncomingHttp is true otherwise No)	
ssl.certificate.ecdsa.fileName	ecdsa private key file name	n/a	Yes (If enableIncomingHttp is true otherwise No)	
ssl.caBundle.k8SecretName	Name of the privatekey secret	n/a	Yes (If enableIncomingHttp is true otherwise No)	
ssl.caBundle.k8NameSpace	Namespace of privatekey	n/a	Yes (If enableIncomingHttp is true otherwise No)	
ssl.caBundle.rsa.fileName	rsa private key file name	n/a	Yes (If enableIncomingHttp is true otherwise No)	
ssl.keyStorePassword.k8SecretName	Name of the privatekey secret	n/a	Yes (If enableIncomingHttp is true otherwise No)	
ssl.keyStorePassword.k8NameSpace	Namespace of privatekey	n/a	Yes (If enableIncomingHttp is true otherwise No)	
ssl.keyStorePassword.fileName	File name that has password for keyStore	n/a	Yes (If enableIncomingHttp is true otherwise No)	

Table 7-12 (Cont.) Ingress Gateway

Name	Description	Default Value	Mandatory	Notes
ssl.trustStorePassword.k8SecretName	Name of the privatekey secret	n/a	Yes (If enableIncomingHttp is true otherwise No)	
ssl.trustStorePassword.k8NameSpace	Namespace of privatekey	n/a	Yes (If enableIncomingHttp is true otherwise No)	
ssl.trustStorePassword.fil eName	File name that has password for trustStore	n/a	Yes (If enableIncomingHttp is true otherwise No)	
uri	Service name of the internal microservice of this NF		Yes	
id	id of the route		Yes	
path	Provide the path to be matched.		Yes	
order	Provide the order of the execution of this route.		Yes	
methodRateLimiting.burstCapacity[0]	burstCapacity		Yes (if routeRateLimiting.enabled)	
methodRateLimiting.refillRate[0]	Refill rate		Yes (if routeRateLimiting.enabled)	
methodRateLimiting.duration[0]	Duration		Yes (if routeRateLimiting.enabled)	
methodRateLimiting.method[0]	Method on which ratelimiting is applicable		Yes (if routeRateLimiting.enabled)	
image.name	Image name of ingress gateway	ocingress_gateway	No	
image.tag	Image Tag name of ingress gateway	1.6.2	No	
image.pullPolicy	Image Pull Policy	Always	No	
initContainersImage.name	Image name of initContainer	configurationinit	No	
initContainersImage.tag	Image tag name of initContainer	1.1.1	No	
initContainersImage.pullPolicy	Image Pull Policy	Always	No	
updateContainersImage.name	Image name of updateContainer	configurationupdate	No	

Table 7-12 (Cont.) Ingress Gateway

Name	Description	Default Value	Mandatory	Notes
updateContainersImage.tag	Image tag name of updateContainer	1.1.1	No	
updateContainersImage.pullPolicy	Image Pull Policy	Always	No	
fullnameOverride	Label to override name of api-gateway micro-service name	ingress	Yes	
serviceMeshCheck	Load balancing will be handled by Ingress gateway, if true it would be handled by serviceMesh	false	Yes	
cipherSuites	Supported Cipher Suites in Ingress	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	No	

Table 7-12 (Cont.) Ingress Gateway

Name	Description	Default Value	Mandatory	Notes
maxRequestsQueuedPerDestination	Jetty Client Settings	1024	No	
maxConnectionsPerDestination	Jetty Client Settings	4 (This will be used when `serviceMeshCheck` is enabled)	No	
maxConnectionsPerIp	Jetty Client Settings	4	No	
connectionTimeout	Jetty Client Settings	10000	No	
ingressGwCertReloadPath		`/ingress-gw/certificate/reload`	No	
ssl.tlsVersion	TLS Version	TLSv1.2	Yes	
ssl.initialAlgorithm		RSA256	Yes	ES256 can also be used, but corresponding certificates need to be used.
resources.limits.cpu	CPU Limit	2		
resources.limits.memory	Memory Limit	4Gi		
resources.limits.initServiceCpu	Init Container CPU Limit	1		
resources.limits.updateServiceCpu	Update Container CPU Limit	1		
resources.limits.initServiceMemory	Init Container Memory Limit	1Gi		
resources.limits.updateServiceMemory	Update Container Memory Limit	1Gi		
resources.requests.cpu	CPU for requests	1		
resources.requests.memory	Memory for requests	2Gi		

Table 7-12 (Cont.) Ingress Gateway

Name	Description	Default Value	Mandatory	Notes
resources.requests.initServiceCpu	Init Container CPU for requests	1		
resources.requests.updateServiceCpu	Update Container CPU for requests	1		
resources.requests.initServiceMemory	Init Container Memory for requests	1Gi		
resources.requests.updateServiceMemory	Update Container Memory for requests	1Gi		
resources.target.averageCpuUtil		80		
minReplicas	Min replicas to scale to maintain an average CPU utilization	2	Yes	
maxReplicas	Max replicas to scale to maintain an average CPU utilization	5	Yes	
log.level.root	Log level for root logs	WARN	No	
log.level.ingress	Log level for ingress logs	INFO	No	
log.level.oauth	Log level for oauth logs	INFO	No	
ports.containerPort	ContainerPort represents a network port in a single container	8081	No	
ports.containersslPort		8443	No	
actuatorPort	ActuatorPort	9090	No	

egress-gw Microservice

Parameter	Description	Mandatory Parameter	Default value
image.repository	Image repository name	Yes	reg-1:5000
image.name	Image name	Yes	ocengress_gateway
image.tag	Tag of Name	Yes	1.7.4

Table 7-13 Egress Gateway

Name	Description	Default Value	Mandatory	Notes
global.appinfoServiceEnable	Enabled to get RBAC permission for k8s apiserver communication	true	Yes	
global.dockerRegistry	Name of the Docker registry which hosts Egress docker images.	ocnrf-registry.us.oracle.com:5000	Yes	Ideally this is the registry which has docker images. Change this value if there is a need.
global.serviceAccountName	Service Account Name	''	No	
serviceEgressGateway.port		8080	No	
serviceEgressGateway.sslPort	SSL Port	8442	No	
serviceEgressGateway.actuatorPort	Actuator Port	9090	No	
enableOutgoingHttps	Enabling it for outgoing https request	false	No	Change it to true for enabling https for outgoing requests.
K8ServiceCheck	Enable this if loadbalancing is to be done by egress instead of K8s	false	No	
scp.scpDefaultScheme	Default scheme applicable when 3gpp-sbi-target-apiroot header is missing	https	No	
scp.scpIntegrationEnabled	Change this to false when scp integration is not required	true	No	
scp.scpRerouteEnabled	Set this flag to true if re-routing to multiple SCP instances is to be enabled.	true	No	
scp.instances.http[0].host	First Scp instance HTTP IP/FQDN	NA	Yes(If "scp.scpIntegrationEnabled" is set to true.)	More SCP instances can be configured in a similar way if required.
scp.instances.http[0].port	First Scp instance Port	NA	Yes(If "scp.scpIntegrationEnabled" is set to true.)	

Table 7-13 (Cont.) Egress Gateway

Name	Description	Default Value	Mandatory	Notes
scp.instances.http[0].apiPrefix	First Scp instance apiPrefix. Change this value to corresponding prefix if "/" is not expected to be provided along. Applicable only for SCP with TLS enabled.	/	No	Examples : XXX, Point to be noted here is that / is not required to be included when providing some data.
scp.instances.https[0].host	First Scp instance HTTPS IP/FQDN	NA	Yes(if "scp.scpIntegrationEnabled" is set to true.)	More SCP instances can be configured in a similar way if required.
scp.instances.https[0].port	First Scp instance HTTPS Port	NA	Yes(if "scp.scpIntegrationEnabled" is set to true.)	
scp.instances.https[0].apiPrefix	First Scp instance apiPrefix. Change this value to corresponding prefix if "/" is not expected to be provided along. Applicable only for SCP with TLS enabled.	/	No	Examples : XXX, Point to be noted here is that / is not required to be included when providing some data.
headlessServiceEnabled	Enabling this will make the service type default to ClusterIP	false	No	
cipherSuites	Supported Cipher Suites in Egress	`TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384` `TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384` `TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256` `TLS_DHE_RSA_WITH_AES_256_GCM_SHA384` `TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256` `TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256`	No	Connection with other ciphers would be rejected.

Table 7-13 (Cont.) Egress Gateway

Name	Description	Default Value	Mandatory	Notes
log.level	Log level	DEBUG	No	
jaegerTracingEnabled	Enable jaeger tracing	false	No	Change it to true if needed.
openTracing.jaeger.udpSender.host	Jaeger Host	jaeger-agent.cne-infra	Yes (If jaegerTracingEnabled is true)	
openTracing.jaeger.udpSender.port	Jaeger Port	6831	Yes (If jaegerTracingEnabled is true)	
openTracing.jaeger.probabilisticSampler		0.5	Yes (If jaegerTracingEnabled is true)	
nrfAuthority	NRF's ${HOSTNAME}:{PORT}	Modify the field with actual value, required if oAuth is enabled.	Yes	
nfType	NFType of service consumer.	Modify the field with actual value , required if oAuth is enabled.	Yes	
nfInstanceId:	NF InstanceId of Service Consumer.	Modify the field with actual value, required if oAuth is enabled.	Yes	
oauthClientEnabled:	Flag to enable or disable oauth client. If not modified, Default value 'false' will be defaulted.	false	No	Change it to true to enable oAuth
consumerPlmnMNC	MNC of service Consumer.	Modify the field with actual value , required if oAuth is enabled.	No	
consumerPlmnMCC	MCC of service Consumer.	Modify the field with actual value , required if oAuth is enabled.	No	

Table 7-13 (Cont.) Egress Gateway

Name	Description	Default Value	Mandatory	Notes
maxRequestsQueuedPerDestination	jetty client configuration	1024	No	
maxConnectionsPerIp	Max Connections allowed per Ip	4	No	
connectionTimeout	Connection timeout in milliseconds	1000	No	
egressGwCertReloadEnabled		true	No	
notificationRateLimit.enabled	Flag to enable rate limiting for "notification" type of messages.	false	No	
notificationRateLimit.duration	Iterations of time duration(In seconds) for which bucketCapacity and refillRate are reset.		Yes(If notificationRateLimit.enabled is set to true)	
notificationRateLimit.bucketCapacity	Holds maximum number of tokens in the bucket for the given duration.		Yes(If notificationRateLimit.enabled is set to true)	
notificationRateLimit.refillRate	Number of tokens to be added to the bucket for the given duration		Yes(If notificationRateLimit.enabled is set to true)	
type	type of service	ClusterIP Possible values are ClusterIP, NodePort, LoadBalancer and ExternalName	Yes	
ssl.privateKey.k8SecretName	Name of the privatekey secret	n/a	Yes (If enableOutgoingHttps is true otherwise No)	
ssl.privateKey.k8NameSpace	Namespace of privatekey	n/a	Yes (If enableOutgoingHttps is true otherwise No)	
ssl.privateKey.rsa.fileName	rsa private key file name	n/a	Yes (If enableOutgoingHttps is true otherwise No)	
ssl.privateKey.ecdsa.fileName	ecdsa private key file name	n/a	Yes (If enableOutgoingHttps is true otherwise No)	

Table 7-13 (Cont.) Egress Gateway

Name	Description	Default Value	Mandatory	Notes
ssl.certificate.k8SecretName	Name of the privatekey secret	n/a	Yes (If enableOutgoingHttps is true otherwise No)	
ssl.certificate.k8NameSpace	Namespace of privatekey	n/a	Yes (If enableOutgoingHttps is true otherwise No)	
ssl.certificate.rsa.fileName	rsa private key file name	n/a	Yes (If enableOutgoingHttps is true otherwise No)	
ssl.certificate.ecdsa.fileName	ecdsa private key file name	n/a	Yes (If enableOutgoingHttps is true otherwise No)	
ssl.caBundle.k8SecretName	Name of the privatekey secret	n/a	Yes (If enableOutgoingHttps is true otherwise No)	
ssl.caBundle.k8NameSpace	Namespace of privatekey	n/a	Yes (If enableOutgoingHttps is true otherwise No)	
ssl.caBundle.rsa.fileName	rsa private key file name	n/a	Yes (If enableOutgoingHttps is true otherwise No)	
ssl.keyStorePassword.k8SecretName	Name of the privatekey secret	n/a	Yes (If enableOutgoingHttps is true otherwise No)	
ssl.keyStorePassword.k8NameSpace	Namespace of privatekey	n/a	Yes (If enableOutgoingHttps is true otherwise No)	
ssl.keyStorePassword.fileName	File name that has password for keyStore	n/a	Yes (If enableOutgoingHttps is true otherwise No)	
ssl.trustStorePassword.k8SecretName	Name of the privatekey secret	n/a	Yes (If enableOutgoingHttps is true otherwise No)	
ssl.trustStorePassword.k8NameSpace	Namespace of privatekey	n/a	Yes (If enableOutgoingHttps is true otherwise No)	

Table 7-13 (Cont.) Egress Gateway

Name	Description	Default Value	Mandatory	Notes
ssl.trustStorePassword.fileName	File name that has password for trustStore	n/a	Yes (If enableOutgoingHttps is true otherwise No)	
resources.limits.cpu	CPU Limit	2		
resources.limits.memory	Memory Limit	4Gi		
resources.limits.initServiceCpu	Init Container CPU Limit	1		
resources.limits.updateServiceCpu	Update Container CPU Limit	1		
resources.limits.initServiceMemory	Init Container Memory Limit	1Gi		
resources.limits.updateServiceMemory	Update Container Memory Limit	1Gi		
resources.requests.cpu	CPU for requests	1		
resources.requests.memory	Memory for requests	2Gi		
resources.requests.initServiceCpu	Init Container CPU for requests	1		
resources.requests.updateServiceCpu	Update Container CPU for requests	1		
resources.requests.initServiceMemory	Init Container Memory for requests	1Gi		
resources.requests.updateServiceMemory	Update Container Memory for requests	1Gi		
resources.target.averageCpuUtil		80		
minReplicas	Minimum replicas to scale to maintain an average CPU utilization	2		

Table 7-13 (Cont.) Egress Gateway

Name	Description	Default Value	Mandatory	Notes
maxReplicas	Maximum replicas to scale to maintain an average CPU utilization	5		
globalretry.enabled	Can be set to true if Scp re-route feature (`scpRerouteEnabled`) is enabled.	false	No	
globalretry.retries	Number of re-routes to be attempted to alternate SCP instances and this property will be considered in the absence of "routesConfig[0].filterName2.retries" attribute at route level.		Yes (If `"routesConfig[0].filterName2.retries"` is not defined)	
routesConfig[0].id	id of the route		Yes	Can be any name of your choice. *Note: Multiple routes can be configured in a similar way.*
routesConfig[0].uri	Provide any dummy url, existing url can also left with existing value		Yes	Please note provided sample url does not make any impact (http or https) as url's will be constructed in the code.
routesConfig[0].path	Provide the path to be matched.		Yes	
routesConfig[0].order	Provide the order of the execution of this route.		Yes	
routesConfig[0].filterName1	Provide filtername as "ScpFilter"		Yes (If scpintegrationenabled is true)	If FilterName1 is not provided then it would be considered as direct Egress Gateway path and configured accordingly during deployment.
routesConfig[0].filterName2.name	Provide filtername as "ScpRetry"		Yes (If scpRerouteEnabled is true)	With out FilterName1 , it is not possible to configure FilterName2.name

Table 7-13 (Cont.) Egress Gateway

Name	Description	Default Value	Mandatory	Notes
routesConfig[0].filterName2.retries	Number of re-routes to be attempted to alternate SCP instances if request matches this route's path.		Yes (If scpRerouteEnabled is true)	If this is not defined then globalretry.retries parameter is applicable when globalretry.enabled is true.
routesConfig[0].filterName2.methods	The type of methods for which the re-route need to be attempted.		Yes (If scpRerouteEnabled is true)	
routesConfig[0].filterName2.statuses	The type response error codes on which the re-route need to be attempted.		Yes (If scpRerouteEnabled is true)	
serviceEgressGateway.port	Internal port on which egress gateway is running for HTTP2	No	8080	Change this value if there is any specific need.
serviceEgressGateway.sslPort	Internal port on which egress gateway is running for HTTPS	No	8442	Change this value if there is any specific need.
deploymentEgressGateway.image	Image name of egress gateway	No	ocegress_gateway	N/A
deploymentEgressGateway.imageTag	Image Tag name of egress gateway	No	1.6.1	N/A
deploymentEgressGateway.pullPolicy	Pull Policy of Image	No	Always	N/A
initContainersImage.name	Image name of initContainer	No	configurationinit	N/A
initContainersImage.tag	Image tag name of initContainer	No	1.1.1	N/A
initContainersImage.pullPolicy	Pull Policy of Image	No	Always	N/A
updateContainersImage.name	Image name of updateContainer	No	configurationupdate	N/A
updateContainersImage.tag	Image tag name of updateContainer	No	1.1.1	N/A

Table 7-13 (Cont.) Egress Gateway

Name	Description	Default Value	Mandatory	Notes
updateContainersImage.pullPolicy	Pull Policy of Image	No	Always	N/A
httpClientBean	To be used when oAuth is enabled. when https is enabled then it should be jettysClient , when https is disabled then it can left as ''	Yes	jettysClient	#Jetty bean name #when http enabled -> '' #when https enabled -> jettysClient
egressGwCertReloadEnabled	Egress GW Certificates Reload Enabled	No	true	N/A
jaegerTracingEnabled	JaegerTracing Enabled	No	false	N/A
ssl.tlsVersion	TLS Version	TLSv1.2	Yes	
initialAlgorithm		RSA256	Yes	ES256 can also be used, but corresponding certificates need to be used.

8
IWF Upgrade

This section includes information about upgrading the existing IWF deployment.

Note: The `ociwf_customized_values.yaml` must be updated with the required details for upgrade.

The `ociwf_customized_values.yaml` can be downloaded from the OHC.

To download the **InterWorking and Mediation Function (IWF) Custom Template** ZIP file from OHC:

- Go to the URL, docs.oracle.com
- Navigate to **Industries>Communications-Diameter Signaling Router-Cloud Native Network Elements**
- Click the **InterWorking and Mediation Function (IWF) Custom Template** link to download the zip file.
- Unzip the template to get `ociwf-custom-values-1.5.0.yaml` file.

To upgrade an existing IWF deployment, execute:

```
helm upgrade <release> -f <ociwf-custom-values-1.5.0.yaml>
```

In case of backout:

1. Check the history of helm deployment:

   ```
   helm history <helm_release>
   ```

2. Rollback to the required revision:

   ```
   helm rollback <release name> <revision number>
   ```

9 IWF Uninstallation

Deleting the IWF deployment

To completely delete or remove the IWF deployment, execute:

```
helm delete --purge <helm-release>
```

For example:

```
helm delete --purge ociwf
```

Delete kubernetes namespace

```
kubectl delete namespace <ociwf kubernetes namespace>
```

For example:

```
kubectl delete namespace iwfsvc
```

10
Troubleshooting IWF

This section provides information to troubleshoot the common error which can be encountered during the installation and upgrade of IWF.

The environment is not working as expected

Problem: The environment is not working as expected.

Solution:

- Check the version of kubectl in system e.g. ‘kubectl version'
- Check if below commands execute successfully:
  - $ kubectl create namespace test
  - $ kubectl delete namespace test
- Check if 'helm version' command works and gives the versions of client and server.

2Debugging of IWF Installation while Installing using helm

Problem: The user is getting the error: *failed to parse ociwf-custom-values-1.5.0.yaml: error converting YAML to JSON: yaml.*

Solution:

Verify the following:

1. The `ociwf-custom-values-1.5.0.yaml` may not be created properly.
2. The tree structure may not be followed.
3. There may be tab spaces in the file.
4. Verify that the `ociwf-custom-values-1.5.0.yaml` is proper

   Refer *Iwf Cloud Native Installation Guide .*
5. If there is no error, helm installation will be deployed.

   Helm status can be checked using following command :

   ```
   helm status <helm release name>
   ```

IWF is not deployed successfully

Problem: The IWF deployment is not successful.

Solution:

1. Verify if IWF specific pods are working as expected by executing the following command:
   `kubectl get pods -n <ociwf_namespace>`

   Check whether all the pods are up and running.

   Sample output:

```
NAME                                     READY STATUS RESTARTS AGE
iwf-pt-mysql-dd8cf7685-tqhm7             1/1   Running   0  3m10s
ociwf-egress-gateway-5d86d7755b-8c4rx    1/1   Running   0  3m10s
ociwf-ingress-gateway-6d5bdcd859-mn2pz   1/1   Running   0  3m10s
ociwf-iwf-configmgr-65957546d5-jfwwr     1/1   Running   0  3m10s
ociwf-iwf-d2h-d6ffd8788-qk52j            1/1   Running   0  3m10s
ociwf-iwf-diameterproxy-56479d8c7-szcwh  1/1   Running   0  3m10s
ociwf-iwf-h2d-6cfff7754d-ppmsk           1/1   Running   0  3m10s
ociwf-iwf-mediation-66fbf5c98f-lzn2j     1/1   Running   0  3m10s
ociwf-iwf-mediation-test-7c5dc59ff5-hsd4p1/1    Running  0  3m10s
ociwf-iwf-pcfdiscovery-67966f7b6b-4rvf4  1/1   Running   2  3m10s
ociwf-nf-mediation-8554fcd55f-wnncw      1/1   Running   0  3m10s
ociwf-nf-mediation-test-5cd6c489fd-86gdh1/1   Running   0  3m10s
ociwf-pcf-diam-gateway-0                 1/1   Running   0  3m10s
```

2. If status of any pod is shown as `ImagePullBackOff` or `ErrImagePull` then it can be due to:
   a. Incorrect ImageName or ImageTag provided in `ociwf-custom-values-1.5.0.yaml`.
      Then, double check the image name and tags in `ociwf-custom-values-1.5.0.yaml`.
   b. Docker registry is incorrectly configured.
      Then, check docker registry is properly configured in all master and slave nodes.
   c. Docker image doesn't exist in the docker repo.
3. If RESTARTS count of the pods is continuously increasing, then it can happen due to the following reasons:
   a. MySQL primary and secondary hosts may not be configured properly in `ociwf-custom-values-1.5.0.yaml`
   b. MySQL servers may not be configured properly according to the pre-installation steps mentioned in *IWF Cloud Native Installation Guide* .

Debugging General CNE

Problem: The environment is not working as expected

Solution:

Execute the command `kubectl get events -n <ociwf_namespace>`to get all the events related to a particular namespace.

Collect the IWF Logs to check the error scenarios

Problem: The error scenarios are checked by collecting the IWF logs or kibana.

Solution:

The following commands must be executed to get the logs from iwf specific pods:

1. Fetch the list of all pods by executing `kubectl get pods -n <ociwf_namespace>`
2. Collect the logs from the pod and redirect to file by executing `kubectl logs <pod_name> -n <ociwf_namespace> > <Log File>`

Example:

use options -f for follow, --tail=1 to only dump the latest logs

A
IWF Yaml Files

This section includes information about configurable parameters defined in IWF Yaml Files.

Sample `ociwf-custom-values-1.5.0.yaml` file:

```
# Copyright 2018 (C), Oracle and/or its affiliates. All rights reserved.
# Default values for iwf-pt.
# This is a YAML-formatted file.
# Declare variables to be passed into your templates

namespace: iwfsvc

#--------------------------------diam-
gateway------------------------------

pcf:
  global:
    dockerRegistry: reg-1:5000
    imageTag: staging-493384
  pcf:
    hostIp: slave1=10.196.46.13
    deploymentOcpmPcfDiamGateway:
      envGatewayMode: bsf
      replicas: 1
      image: diam-gateway
      imageTag: 1.5.0
      nodeSelectorEnabled: false
      nodeSelectorKey: nftype
      nodeSelectorValue: ociwf


#---------------------------------
mysql--------------------------------------
iwf-mysql:
  enabled: true
  nodeSelectorEnabled: false
  nodeSelectorKey: nftype
  nodeSelectorValue: ociwf
  mysqlUser: iwfusr
  mysqlPassword: Dukw1@m?
  initializationFiles:
   iwf-db.sql: |-
      CREATE DATABASE IF NOT
EXISTS iwfdb DEFAULT CHARACTER SET utf8 DEFAULT COLLATE utf8_general_ci;
   permission.sql: |-
      GRANT ALL PRIVILEGES ON *.* TO 'iwfusr'@'%';

#---------------------------------dp---------------------------------
```

```
iwf-diameterproxy:
  replicaCount: 1
  image:
    repository: reg-1:5000
    name: ociwf-iwfdiamproxy
    tag: 1.5.0
  DIAMETER_Realm: ociwf.oracle.com
  DIAMETER_Identity: iwf.ociwf.oracle.com
  dpDBService1: iwf-pt-mysql-svc
  dpDBService2: iwf-pt-mysql-svc
  opentracingHost: 10.75.157.169
  opentracingPort: 32460
  mysqlUsername: iwfusr
  mysqlPassword: Dukw1@m?
  pcfDiscoveryMode: true
  connectorMode: bsf
  service:
    nodeSelectorEnabled: false
    nodeSelectorKey: nftype
    nodeSelectorValue: ociwf


#-----------------------------------
d2h-----------------------------------

iwf-d2h:
  replicaCount: 1
  image:
    repository: reg-1:5000
    name: ociwf-iwfd2h
    tag: 1.5.0
  opentracingHost: 10.75.157.169
  opentracingPort: 32460
  service:
    nodeSelectorEnabled: false
    nodeSelectorKey: nftype
    nodeSelectorValue: ociwf



#-----------------------------------
h2d-----------------------------------

iwf-h2d:
  replicaCount: 1
  image:
    repository: reg-1:5000
    name: ociwf-iwfh2d
    tag: 1.5.0

  opentracingHost: 10.75.157.169
  opentracingPort: 32460
  service:
    nodeSelectorEnabled: false
```

```
    nodeSelectorKey: nftype
    nodeSelectorValue: ociwf


#----------------------------------
mediation-----------------------------------

iwf-mediation:
  replicaCount: 1
  replicaCountMedTest: 1
  enabled: true
  image:
    repository: reg-1:5000
    name: ocmed-iwfmediation
    tag: 1.5.0

  service:
    active:
      nodePortHttp: 30079
      nodePortHttps: 30080
      forwardToTest: false
      nodeSelectorEnabled: false
      nodeSelectorKey: nftype
      nodeSelectorValue: ociwf

  jaegerTracingEnabled: false
  bodyInTraceEnabled: false
  openTracing:
    jaeger:
      udpSender:
        host: "jaeger-agent.cne-infra"
        port: 6831
      logSpans: false
      probabilisticSamplingRate: 0.5

  log:
    active: INFO
    test: INFO
  # Enables
pegging of rule based metrics::Acceptable values(true/false)
  ruleMetricsEnable: false
  nfInstanceId: IWF1

#----------------------------------
mediation-----------------------------------
nf-mediation:
  enabled: true
  image:
    repository: reg-1:5000
    name: ocmed-nfmediation
    tag: 1.5.0

  service:
    active:
      nodePortHttp: 30081
```

```
      nodePortHttps: 30082
      forwardToTest: false
      corePoolSize: 34
      maxPoolSize: 66
      queueCapacity: 10000
      nodeSelectorEnabled: false
      nodeSelectorKey: nftype
      nodeSelectorValue: ociwf

  jaegerTracingEnabled: false
  bodyInTraceEnabled: false
  openTracing:
    jaeger:
      udpSender:
        host: "jaeger-agent.cne-infra"
        port: 6831
      logSpans: false
      probabilisticSamplingRate: 0.5

  log:
    active: INFO
    test: INFO
  # Enables
pegging of rule based metrics::Acceptable values(true/false)
  ruleMetricsEnable: false
  nfInstanceId: IWF1

#---------------------------------
nrfclient---------------------------------------
nrfclient:
  global:
    nrfClientEnable: false
    envJaegerAgentHost: ''
    envJaegerAgentPort: 6831
    nrfClientNodePort: 0
    dockerRegistry: ocnrf-registry.us.oracle.com:5000
    imageServiceDetector: nrf-client/readiness-detector:latest
    configServerEnable: true
    configServerFullNameOverride: ocpm-config
    envMysqlHost: iwf-pt-mysql-svc
    envMysqlPort: '3306'
    dbCredSecretName: 'iwf-mysql-login'
    appinfoServiceEnable: false
    performanceServiceEnable: false
    deploymentNrfClientService:
      envNfNamespace: 'iwfsvc'
      envNfType: 'iwf'
      envConsumeSvcName: 'appinfo'
      envEgressGatewayFullnameOverride: egress-gateway
      envEgressGatewayPort: "8080"
      nfApiRoot: http://ocnrf-ingressgateway.ocnrf:80
      nodeSelectorEnabled: false
      nodeSelectorKey: nftype
      nodeSelectorValue: ociwf
  perf-info:
```

```
  service_namespace: iwfsvc
  replicaCount: 1
  image: perf_info
  imageTag: 1.5.0
  imagepullPolicy: Always
  nodeSelectorEnabled: false
  nodeSelectorKey: nftype
  nodeSelectorValue: ociwf
  service:
    type: ClusterIP
    port: 5905
  resources: {}
  nodeSelector: {}
  tolerations: []
  affinity: {}
  ingress:
    enabled: false
  configmapPerformance:
    prometheus: http://prometheus-server.prometheus:5802
nrf-client:
  configmapApplicationConfig:
     profile: |-
       [appcfg]
       primaryNrfApiRoot=http://10.178.246.40:30707
       secondaryNrfApiRoot=
       retryAfterTime=PT120S
       nrfClientType=CUSTOM_IWF
       nrfClientSubscribeTypes=BSF
       appProfiles=[{}]
       enableF3=true
       enableF5=true
       renewalTimeBeforeExpiry=3600
       validityTime=30
       enableSubscriptionAutoRenewal=true
       acceptAdditionalAttributes=false
       retryForCongestion=5

  nrf-client-nfdiscovery:
    image: nrf-client
    imageTag: '1.2.2'
    envJaegerSamplerParam: '1'
    envJaegerSamplerType: ratelimiting
    envJaegerServiceName: nrf-client-nfdiscovery
    cpuRequest: 2
    cpuLimit: 2
    memoryRequest: 1Gi
    memoryLimit: 1Gi
    minReplicas: 1
    maxReplicas: 1
    averageCpuUtil: 80
    type: ClusterIP
    cacheDiscoveryResults: true

  nrf-client-nfmanagement:
    image: nrf-client
```

```
      imageTag: '1.2.2'
      envJaegerSamplerParam: '1'
      envJaegerSamplerType: ratelimiting
      envJaegerServiceName: nrf-client-nfmanagement
      replicas: 0
      cpuRequest: 1
      cpuLimit: 1
      memoryRequest: 1Gi
      memoryLimit: 1Gi
      type: ClusterIP

  config-server:
    enabled: false
    fullNameOverride: "config-server"
    image: config_server
    imageTag: 1.5.0
    envJaegerServiceName: pcf-config
    envMysqlDatabase: iwfdb
    replicas: 0
    nodeSelectorEnabled: false
    nodeSelectorKey: nftype
    nodeSelectorValue: ociwf
    cpuRequest: 0.5
    cpuLimit: 8
    memoryLimit: 2Gi
    memoryRequest: 1Gi
    servicePcfConfig:
      type: NodePort
    nodeSelectorEnabled: false
    nodeSelectorKey: nftype
    nodeSelectorValue: ociwf


  appinfo:
    enabled: true
    image: app_info
    imageTag: 1.5.1
    replicas: 1
    debug: true
    serviceAccountName: ''
    categoryCoreServices: "nrf:ocnrf-nfregistration"
    nodeSelectorEnabled: false
    nodeSelectorKey: nftype
    nodeSelectorValue: ociwf


#----------------------------------
pcfDiscovery-----------------------------------

iwf-pcfdiscovery:
  replicaCount: 1
  image:
    repository: reg-1:5000
    name: ociwf-iwfpcfdiscovery
    tag: 1.5.0
```

```
  service:
    nodeSelectorEnabled: false
    nodeSelectorKey: nftype
    nodeSelectorValue: ociwf


  opentracingHost: 10.75.157.169
  opentracingPort: 32460
  bsfSvc: bsf-stub-service.default
  bsfPort: 8080
  nfDiscoverySvc: ociwf-nrf-client-nfdiscovery
  #The port
is nrf-client-nfdiscovery port used to forward query to nrf-client
  nfDiscoveryPort: 5910
  #Use CUSTOM_IWF with Oracle NRF, else use AF
  #ensure that
CUSTOM_IWF is present in allowed NF list for BSF entry in NRF
  requesterNfType: CUSTOM_IWF
  targetNfType: BSF

#----------------------------Ingress
gateway-----------------------------------------------

ingress-gateway:
  global:
    # Docker registry name
    dockerRegistry: ocnrf-registry.us.oracle.com:5000
    serviceAccountName: ''
    nodeSelector:
      nodeKey: ''
      nodeValue: ''

    #Specify type of service - Possible
values are :- ClusterIP, NodePort, LoadBalancer and ExternalName
    type: LoadBalancer
    # Config-Server
Service. Shall be used as {{ ReleaseName }}-configServerFullNameOverride
    configServerFullNameOverride: ocpm-config
  image:
    # image name
    name: ocingress_gateway
    # tag name of image
    tag: 1.7.4
    # Pull Policy - Possible Values are:- Always, IfNotPresent, Never
    pullPolicy: Always

  initContainersImage:
    # inint Containers image name
    name: configurationinit
    # tag name of init Container image
    tag: 1.2.0
    # Pull Policy - Possible Values are:- Always, IfNotPresent, Never
    pullPolicy: Always

  updateContainersImage:
```

```
  # update Containers image name
  name: configurationupdate
  # tag name of update Container image
  tag: 1.2.0
  # Pull Policy - Possible Values are:- Always, IfNotPresent, Never
  pullPolicy: Always

service:
  ssl:
    privateKey:
      k8SecretName: ociwf-secret
      k8NameSpace: iwfsvc
      rsa:
        fileName: rsa_private_key_pkcs1.pem
      ecdsa:
        fileName: ssl_ecdsa_private_key.pem

    certificate:
      k8SecretName: ociwf-secret
      k8NameSpace: iwfsvc
      rsa:
        fileName: tmp.cer
      ecdsa:
        fileName: ssl_ecdsa_certificate.crt

    caBundle:
      k8SecretName: ociwf-secret
      k8NameSpace: iwfsvc
      fileName: caroot.cer

    keyStorePassword:
      k8SecretName: ociwf-secret
      k8NameSpace: iwfsvc
      fileName: key.txt

    trustStorePassword:
      k8SecretName: ociwf-secret
      k8NameSpace: iwfsvc
      fileName: trust.txt
  nodeSelectorEnabled: false
  nodeSelectorKey: nftype
  nodeSelectorValue: ociwf


ports:
  # ContainerPort represents a network port in a single container
  containerPort: 8081
  containersslPort: 8443
  actuatorPort: 9090

#Set the root log level
log:
  level:
    root: WARN
    ingress: WARN
```

```
    oauth: WARN
  traceIdGenerationEnabled: true

# Resource details
resources:
  limits:
    cpu: 2
    initServiceCpu: 1
    updateServiceCpu: 1
    memory: 4Gi
    updateServiceMemory: 1Gi
    initServiceMemory: 1Gi
  requests:
    cpu: 2
    initServiceCpu: 1
    updateServiceCpu: 1
    memory: 2Gi
    updateServiceMemory: 1Gi
    initServiceMemory: 1Gi
  target:
    averageCpuUtil: 80

# Number of Pods must always be available, even during a disruption.
minAvailable: 1
# Min replicas to scale to maintain an average CPU utilization
minReplicas: 1
# Max replicas to scale to maintain an average CPU utilization
maxReplicas: 1

# enable jaeger tracing
jaegerTracingEnabled: false

#OAUTH CONFIGURATION
oauthValidatorEnabled: false
nfType: SMF
nfInstanceId: 6faf1bbc-6e4a-4454-a507-a14ef8e1bc11
producerScope: nsmf-pdusession,nsmf-event-exposure
allowedClockSkewSeconds: 0
nrfPublicKeyKubeSecret: nrfpublickeysecret
nrfPublicKeyKubeNamespace: ocegress
validationType: strict
producerPlmnMNC: 123
producerPlmnMCC: 346


##########################################################################
# To Initialize SSL related infrastructure in init/update container
initssl: true
#Server Configuration for http and https support
enableIncomingHttp: true
enableIncomingHttps: false
enableOutgoingHttps: false
needClientAuth: false

##########################################################################
```

```
  serviceMeshCheck: false
  #Below field is used for blacklisting(removing) a request header
at global level. Hence, it will be applied to all routes configured.
  globalRemoveRequestHeader:
  - name: myheader4  #Change the value to the reqeust header name which
you want removed from all requests which match to any route configured.
  #Below field is used for blacklisting(removing) a response header
at global level. Hence, it will be applied to all routes configured.
  globalRemoveResponseHeader:
  - name:
myresponseheader2  #Change the value to the response header name which
you want removed from all responses which match to any route configured.

  routesConfig:
  - id: nfmediation
    uri: http://ociwf-nf-mediation:9090/
    path: /nmediation-http/v1/**
    order: 1
    filters:
#      addRequestHeader: # specify what headers you need to add
#      - name: X-Forwarded-Proto
#        value: http
      methodRateLimiting:
# specify the list of methods u have to rate limit
      - method: POST
        burstCapacity: 1
        refillRate: 1
        duration: 1 # in seconds
      - method: GET
        burstCapacity: 1
        refillRate: 1
        duration: 9 # in seconds
    #Below field
is used for blacklisting(removing) a request header at route level.
    removeRequestHeader:
    - name: myheader1
    - name: myheader3
    #Below field
is used for blacklisting(removing) a response header at route level.
    removeResponseHeader:
    - name: myresponseheader1
    - name: myresponseheader3

  - id: iwfmediation
    uri: http://ociwf-iwf-mediation:9090/
    path: /**
    order: 1
    filters:
#      addRequestHeader: # specify what headers you need to add
#      - name: X-Forwarded-Proto
#        value: https
      methodRateLimiting:
# specify the list of methods u have to rate limit
      - method: POST
        burstCapacity: 1
```

```
        refillRate: 1
        duration: 1 # in seconds
      - method: GET
        burstCapacity: 1
        refillRate: 1
        duration: 9 # in seconds
    #Below field
is used for blacklisting(removing) a request header at route level.
    removeRequestHeader:
    - name: myheader1
    - name: myheader3
    #Below field
is used for blacklisting(removing) a response header at route level.
    removeResponseHeader:
    - name: myresponseheader1
    - name: myresponseheader3


  #Jetty Client settings
  maxConcurrentPushedStreams: 1000
  maxRequestsQueuedPerDestination: 5000
  #Below value will be used when serviceMeshCheck is enabled
  maxConnectionsPerDestination: 4
  maxConnectionsPerIp: 4
  connectionTimeout: 10000 #(ms)
  requestTimeout: 1000 #(ms)


#----------------------------Egress
gateway-----------------------------------------------

egress-gateway:
  #Enabled to get RBAC permission for k8s apiserver communication
  global:
    appinfoServiceEnable: true
    dockerRegistry: ocnrf-registry.us.oracle.com:5000
    serviceAccountName: ''
    nodeSelector:
      nodeKey: ''
      nodeValue: ''

  serviceEgressGateway:
    port: 8080
    sslPort: 8442
    actuatorPort: 9090
    nodeSelectorEnabled: false
    nodeSelectorKey: nftype
    nodeSelectorValue: ociwf

  deploymentEgressGateway:
    image: ocegress_gateway
    imageTag: 1.7.4
    pullPolicy: Always

  initContainersImage:
```

```
    name: configurationinit
    tag: 1.2.0
    pullPolicy: Always

  updateContainersImage:
    name: configurationupdate
    tag: 1.2.0
    pullPolicy: Always


  #HTTPS Configuration#####################
  #
  initssl: true
  enableIncomingHttps: false
  #enable true only if "initssl" --> true
  enableOutgoingHttps: false
  ##########################################

  #Enabling this will make the service type default to ClusterIP
  headlessServiceEnabled: false

  ports:
    containerPort: 8080

  log:
    level:
      root: WARN
      egress: INFO
      oauth: INFO

  service:
    # Specify type of service - Possible
values are :- ClusterIP, NodePort, LoadBalancer and ExternalName
    type: ClusterIP
    ssl:
      #supportedCipherSuiteList: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
      privateKey:
        k8SecretName: ociwf-secret
        k8NameSpace: iwfsvc
        rsa:
          fileName: rsa_private_key_pkcs1.pem
        ecdsa:
          fileName: ssl_ecdsa_private_key.pem

      certificate:
        k8SecretName: ociwf-secret
        k8NameSpace: iwfsvc
        rsa:
          fileName: tmp.cer
        ecdsa:
          fileName: ssl_ecdsa_certificate.crt

      caBundle:
        k8SecretName: ociwf-secret
        k8NameSpace: iwfsvc
```

```
      fileName: caroot.cer

    keyStorePassword:
      k8SecretName: ociwf-secret
      k8NameSpace: iwfsvc
      fileName: key.txt

    trustStorePassword:
      k8SecretName: ociwf-secret
      k8NameSpace: iwfsvc
      fileName: trust.txt

# Resource details
resources:
  limits:
    cpu: 2
    initServiceCpu: 1
    updateServiceCpu: 1
    memory: 4Gi
    updateServiceMemory: 1Gi
    initServiceMemory: 1Gi
  requests:
    cpu: 1
    initServiceCpu: 1
    updateServiceCpu: 1
    memory: 2Gi
    updateServiceMemory: 1Gi
    initServiceMemory: 1Gi
  target:
    averageCpuUtil: 80

# Number of Pods must always be available, even during a disruption.
minAvailable: 1
# Min replicas to scale to maintain an average CPU utilization
minReplicas: 1
# Max replicas to scale to maintain an average CPU utilization
maxReplicas: 1

nrfAuthority: 10.75.224.7:8085
nfType: PCF
nfInstanceId: fe7d992b-0541-4c7d-ab84-c6d70b1b01b1
#Enable OAUTH client
oauthClientEnabled: false
#Jetty bean name
#when http enabled -> ''
#when https enabled -> jettysClient
httpClientBean: ''

# Overrides  the given string instead of chart name
#fullnameOverride: egress

notificationRateLimit:
  enabled: true
  duration: 1
  bucketCapacity: 1
```

```
    refillRate: 1

  #jetty client configuration
  maxConcurrentPushedStreams: 1000
  maxRequestsQueuedPerDestination: 5000
  #maxConnectionsPerDestination: 4
  maxConnectionsPerIp: 4
  connectionTimeout: 10000 #(ms)
  requestTimeout: 1000 #(ms)


  egressGwCertReloadEnabled: true
  egressGwCertReloadPath: /egress-gw/store/reload

  # enable jaeger tracing
  jaegerTracingEnabled: false


#----------------------------------------Config-
Mgr----------------------------

iwf-configmgr:
  replicaCount: 1
  image:
    repository: reg-1:5000
    name: ociwf-iwfconfigmgr
    tag: 1.5.0
    pullPolicy: IfNotPresent

  mysqlUsername: iwfusr
  mysqlPassword: Dukw1@m?
  mysqlService: iwf-pt-mysql-svc

  service:
    nodeSelectorEnabled: false
    nodeSelectorKey: nftype
    nodeSelectorValue: ociwf
```