Oracle® Communications

Security Edge Protection Proxy (SEPP) Cloud Native Installation Guide

Release 1.3.0

F30628-02

June 2020

ORACLE

Oracle Communications Security Edge Protection Proxy (SEPP) Cloud Native Installation Guide, Release 1.3.0

F30628-02

Contents

List of Tables

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

Oracle Communications Security Edge Protection Proxy (OCSEPP) supports IPX Proxy mode with modification policy.

1 Overview

Oracle Communication Security Edge Protection Proxy (OCSEPP) is a proxy network functions (NF) which is used for secured communication between inter-Public Land Mobile Network (PLMN) messages. This document provides a brief overview of the recommended methods for installing SEPP.

Oracle SEPP is deployed by both Mobile Network Operators (MNO) and Internetwork Packet Exchange (IPX) providers. MNOs deploy OCSEPP acting as 3GPP 5GC SEPP NF which enables inter PLMN communication between two networks via N32 interface.IPX providers shall deploy OCSEPP acting as IPX Proxy enabling inter PLMN communication between MNO's through N32 interface supporting Application Layer Security (ALS) as specified in TS 33.501. IPX provider is able to deploy OCSEPP in either of one mode i.e. functionality of 5GC SEPP NF or IPX proxy. IPX providers are able to host 5GC SEPP NF functionality for few of the MNO's and host IPX proxy functionality for rest of the MNOs.

For more details on SEPP Architecture, refer to SEPP User's Guide.

Reference

Following is the reference document:

1. Cloud Native Environment 1.4 Installation Document

Acronyms

Table 1-1 Acronyms

Acronym	Meaning
ALS	Application Layer Security
CRD	Custom Resource Definition
CNE	Cloud Native Environment
DNS	Domain Name System
FQDN	Fully Qualified Domain Name
IPX	Internetwork Packet Exchange
JWS	JSON Web Service
NF	Network Function
MNO	Mobile Network Operator
OHC	Oracle Help Center
OSDC	Oracle Software Delivery Cloud
PLMN	Public Land Mobile Network
SEPP	Security Edge Protection Proxy
SVC	Services
TLS	Transport Layer Security

2
Installing SEPP

This chapter describes how to install SEPP on a Cloud Native Environment (CNE).

Prerequisites

The 5G SEPP requires the following environment:

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

The following software must be installed:

Software	Version
Kubernetes	v1.15.3
HELM	v2.14.3

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

Software	Chart Version	Notes
elasticsearch	5.5.4	Needed for Logging Area
elastic-curator	5.5.4	Needed for Logging Area
elastic-exporter	1.0.2	Needed for Logging Area
logs	2.0.7	Needed for Logging Area
kibana	6.7.0	Needed for Logging Area
grafana	6.1.6	Needed for Metrics Area
prometheus	9.1.2	Needed for Metrics Area
prometheus-node-exporter	0.17.0	Needed for Metrics Area
metallb	0.7.3	Needed for External IP
metrics-server	0.3.1	Needed for Metric Server
tracer	0.8.3	Needed for Tracing Area

> **Note:**
>
> Install the specified software items before proceeding, if any of the above services are needed and the respective software is not already installed in CNE.
> To check the installed software items, execute:
>
> ```
> helm ls
> ```
>
> Use the helm command with `admin.conf` file, if requried:
>
> ```
> helm --kubeconfig admin.conf
> ```

Installation Sequence

This section provides the procedure in which SEPP must be installed.

Creating namespace

Following is the procedure to create the namespace and verify it.

1. Execute the following command to create namespace:

   ```
   $ kubectl create namespace <required namespace>
   ```

   Example:

   ```
   $ kubectl create namespace seppsvc
   ```

Creating secrets for enabling HTTPS

Creation of secrets for enabling HTTPS in OCSEPP ocegress gateway

This section explains the steps to create secret for HTTPS related details. This section must be executed before enabling HTTPS in OCSEPP Egress gateway.

> **Note:**
>
> The passwords for TrustStore and KeyStore are stored in respective password files below.

To create kubernetes secret for HTTPS, following files are required:-

- ECDSA private key and CA signed certificate of OCSEPP (if initialAlgorithm is ES256)
- RSA private key and CA signed certificate of OCSEPP (if initialAlgorithm is RSA256)

- TrustStore password file
- KeyStore password file
- CA certificate

> **Note:**
>
> Creation process for private keys, certificates and passwords is on discretion of user/operator.

1. Execute the following command to create secret:

```
$ kubectl create secret generic <ocegress-secret-name> --
fromfile=<ssl_ecdsa_private_key.pem> --from-
file=<rsa_private_key_pkcs1.pem> --fromfile=<ssl_truststore.txt> --from-
file=<ssl_keystore.txt> --from-file=<caroot.cer> --
fromfile=<ssl_rsa_certificate.crt> --from-
file=<ssl_ecdsa_certificate.crt> -n <Namespace of OCSEPP ocegress
Gateway secret>
```

> **Note:**
>
> Note down the command used during the creation of kubernetes secret, this command will be used for updates in future.

Example: The names used below are same as provided in custom values.yaml in OCSEPP deployment.

```
$ kubectl create secret generic ocegress-secret --
fromfile=ssl_ecdsa_private_key.pem --from-
file=rsa_private_key_pkcs1.pem --fromfile=ssl_truststore.txt --from-
file=ssl_keystore.txt --from-file=caroot.cer --
fromfile=ssl_rsa_certificate.crt --from-file=ssl_ecdsa_certificate.crt -
n ocsepp
```

2. Verify the secret created using the following command:

```
$ kubectl describe secret <ocegress-secret-name> -n <Namespace of
OCSEPP ocegress Gateway secret>
```

Example:

```
$ kubectl describe secret ocegress-secret -n ocsepp
```

Creating secret for n32flpx

Following is the procedure to create secret for N32f-IPX:

1. Execute the following command to create a ECDSA private key with p256 curve:

   ```
   openssl ecparam -name prime256v1 -genkey -noout -out
   ecdsa_private_key.pem
   ```

2. Execute the following command to convert the private key in .pem format and also in PKCS8 Encoded:

   ```
   openssl pkcs8 -topk8 -nocrypt -in private.key -outform pem -out
   ecdsa_private_key_pkcs8.pem
   ```

3. Execute the following command to create the secret for that private key:

   ```
   kubectl create secret generic ocsepp-ipx-secret --from-
   file=ecdsa_private_key_pkcs8.pem -n seppsvc
   ```

Installation Tasks

This section describes the tasks that the user needs to follow for installing SEPP.

Following is the procedure to install SEPP:

1. Login to MOS using the appropriate login credentials.
2. Select **Product & Updates** tab.
3. In **Patch Search** console select **Product or Family (Advanced)** tab.
4. Enter *Oracle Communications Cloud Native Core - 5G* in **Product** field and select the product from the Product drop-down.
5. Select *Oracle Communications Cloud Native Security Edge Protection Proxy <release_number>* in **Release** field.
6. Click **Search**. The **Patch Advanced Search Results** list appears.
7. Select the required patch from the list. The Patch Details window appears.
8. Click on **Download**. File Download window appears.
9. Click on the **<p********_<release_number>_Tekelec>.zip** file.
10. Click on the zip file to download the network function patch.
11. Unzip the file to the system where you want to install the network function. You can find the SEPP package as follows:
    `ReleaseName-pkg-Releasenumber.tgz`

    where:
    ReleaseName is a name which is used to track this installation instance.

    Releasenumber is the release number.

    For example, ocsepp-pkg-1.3.0.0.0.tgz
12. Untar the SEPP package file to get SEPP docker image tar file:

    ```
    tar -xvzf ReleaseName-pkg-Releasenumber.tgz
    ```

13. Load the *ocsepp-images-<release_number>.tar* file into the Docker system:

    ```
    docker load --input /IMAGE_PATH/ocsepp-images-<release_number>.tar
    ```

14. Verify that the image is loaded correctly by entering this command:

    ```
     docker images
    ```

15. 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>
    ```

16. Untar the helm files:

    ```
    tar -xvzf ocsepp-<release_number>.tgz
    ```

17. Create the customize ocsepp-custom-values-1.3.0.yaml file with the required input parameters. To customize the file, refer to <customization chapter>
18. Go to the extracted OCSEPP package as explained in:

    ```
    cd ocsepp-<release_number>
    ```

19. Install OCSEPP by executing the following command:

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

3
Customizing SEPP

This section explains the configuration parameters of the SEPP.

Follow the below steps to customize the `ocsepp-custom-values-1.3.0.yaml` file as per the required parameters:

1. Go to the Oracle Help Center (OHC) Web site.
2. Navigate to **Industries->Communications->Cloud Native Core->Release 2.2.0**.
3. Click the **SEPP Custom Template** link to download the zip file.
4. Unzip the file to get ocscp-custom-configTemplates-1.3.0.0.0 file that contains the ocsepp-custom-configTemplates-1.3.0.0.0. This file is used during installation.
5. Customize the ocsepp-custom-values-1.3.0.yaml file.
6. Save the updated ocsepp-custom-values-1.3.0.yaml file in the helm chart directory.

Configuration Parameters

This section includes information about the configuration parameters of OCSEPP.

OCSEPP allows customization of parameters for the following services and related settings.

Global Parameters: Ingress Gateway

Table 3-1 Global Parameters: Ingress Gateway

Parameter	Description	Mandatory Parmeter	Default value	Notes
global.dockerRegistry	Name of the Docker registry which hosts Ingress docker images.	Yes	reg-1:5000	This is the registry which has docker images. Change this value if there is a need.
global.type	type of service	Yes	LoadBalancer	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	No	true	

Table 3-1 (Cont.) Global Parameters: Ingress Gateway

Parameter	Description	Mandatory Parmeter	Default value	Notes
global.metalLbIpAllocationAnnotation	Address Pool Annotation for Metallb	No	metallb.universe.tf/address-pool: signaling	
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	No	false	
global.staticIpAddress	StaticIp		10.75.212.60	
global.publicHttpSignalingPort	Http Signalling port	Yes	80	
global.publicHttpsSignallingPort	Https Signalling port	Yes	443	
global.staticNodePortEnabled	Node Port Enabled	No	true	
global.staticHttpNodePort	Http Node Port	Yes	30075	
global.staticHttpsNodePort	Https Node Port	Yes	30043	
enableOutgoingHttps	Enabling it for outgoing https request	Yes	false	Change it to true for enabling https for outgoing requests.
enableIncomingHttp	Enabling it for incoming http request	Yes	false	
enableIncomingHttps	Enabling it for incoming https request	Yes	true	
oauthValidatorEnabled	Oauth Validator Enabled	Yes	false	Change it to true to enable oauth
jaegerTracingEnabled	Enable jaeger tracing	No	false	Change it to true if needed.
openTracing.jaeger.udpSender.host	Jaeger Host	Yes (If jaegerTracingEnabled is true)	jaeger-agent.cne-infra	

Table 3-1 (Cont.) Global Parameters: Ingress Gateway

Parameter	Description	Mandatory Parmeter	Default value	Notes
openTracing.jaeger.udpSender.port	Jaeger Port	Yes (If jaegerTracingEnabled is true)	6831	
openTracing.jaeger.probabilisticSampler		Yes (If jaegerTracingEnabled is true)	0.5	
nfType	NFType of service producer	Yes (When oauthValidatorEnabled)	Value to be updated accordingly	
nfInstanceId:	NF InstanceId of service producer.	Yes (When oauthValidatorEnabled)	Value to be updated accordingly	
producerScope:	Comma-seperated list of services hosted by service producer.	Yes (When oauthValidatorEnabled)	Value to be updated accordingly	
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.	Yes (When oauthValidatorEnabled)	0	
nrfPublicKeyKubeSecret	Name of the secret which stores the public key(s) of NRF.	Yes (When oauthValidatorEnabled)	Value to be updated accordingly	
nrfPublicKeyKubeNamespace	Namespace of the NRF publicKey Secret	Yes (When oauthValidatorEnabled)	Value to be updated accordingly	

Table 3-1 (Cont.) Global Parameters: Ingress Gateway

Parameter	Description	Mandatory Parmeter	Default value	Notes
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 doesnot contain "Authorization" header, validation will be ignored.	Yes (When oauthValidatorEnabled)	Value to be updated accordingly	
producerPlmnMNC	MNC of service producer.	No	Value to be updated accordingly	
producerPlmnMCC	MCC of service producer.	No	Value to be updated accordingly	

Global Parameters: Egress Gateway

Table 3-2 Global Parameters: Egress Gateway

Parameter	Description	Mandatory Parameters	Dafault Value	Notes
ssl.tlsVersion	Indicate the version of TLS used.	Yes(If enableIncomingHttp is true otherwise No)	TLSv1.2	
ssl.privateKey.k8SecretName	Name of the privatekey secret	Yes (If enableIncomingHttp is true otherwise No)	n/a	
ssl.privateKey.k8NameSpace	Namespace of privatekey	Yes (If enableIncomingHttp is true otherwise No)	n/a	

Table 3-2 (Cont.) Global Parameters: Egress Gateway

Parameter	Description	Mandatory Parameters	Dafault Value	Notes
ssl.privateKey.rsa.fileName	rsa private key file name	Yes (If enableIncomingHttp is true otherwise No)	n/a	
ssl.privateKey.ecdsa.fileName	ecdsa private key file name	Yes (If enableIncomingHttp is true otherwise No)	n/a	
ssl.certificate.k8SecretName	Name of the privatekey secret	Yes (If enableIncomingHttp is true otherwise No)	n/a	
ssl.certificate.k8NameSpace	Namespace of privatekey	Yes (If enableIncomingHttp is true otherwise No)	n/a	
ssl.certificate.rsa.fileName	rsa private key file name	Yes (If enableIncomingHttp is true otherwise No)	n/a	
ssl.certificate.ecdsa.fileName	ecdsa private key file name	Yes (If enableIncomingHttp is true otherwise No)	n/a	
ssl.caBundle.k8SecretName	Name of the privatekey secret	Yes (If enableIncomingHttp is true otherwise No)	n/a	
ssl.caBundle.k8NameSpace	Namespace of privatekey	Yes (If enableIncomingHttp is true otherwise No)	n/a	

Table 3-2 (Cont.) Global Parameters: Egress Gateway

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

Table 3-3 Resource Customizable Parameters

Parameter	Description	Mandatory Parameters	Dafault Value	Notes
resources.limits.cpu	CPU Limit		2	Change all the values as per the need

Table 3-3 (Cont.) Resource Customizable Parameters

Parameter	Description	Mandatory Parameters	Dafault Value	Notes
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	Min replicas to scale to maintain an average CPU utilization	Yes	2	
maxReplicas	Max replicas to scale to maintain an average CPU utilization	Yes	5	
log.level	Log level	No	DEBUG	
ports.containerPort	ContainerPort represents a network port in a single container	No	8081	
ports.containersslPort		No	8443	
actuatorPort	ActuatorPort	No	9090	

Table 3-4 Routes Config Customizable Parameters

Parameter	Description	Mandatory Parameters	Dafault Value	Notes
id	id of the route	Yes	n32f-ipx	
uri	Service name of the internal microservice of this NF	Yes	http://ocsepp-n32f-ipx:8082/	
path	Provide the path to be matched.	Yes	/n32f-forward/v1/n32f-process	
order	Provide the order of the execution of this route.	Yes	1	

Table 3-5 Fixed value parameters

Parameter	Description	Mandatory Parameters	Dafault Value	Notes
image.name	Image name of ingress gateway	No	ocingress_gateway	
image.tag	Image Tag name of ingress gateway	No	1.6.2	
image.pullPolicy	Image Pull Policy	No	Always	
initContainersImage.name	Image name of initContainer	No	configurationinit	
initContainersImage.tag	Image tag name of initContainer	No	1.1.1	
initContainersImage.pullPolicy	Image Pull Policy	No	Always	
updateContainersImage.name	Image name of updateContainer	No	configurationupdate	
updateContainersImage.tag	Image tag name of updateContainer	No	1.1.1	
updateContainersImage.pullPolicy	Image Pull Policy	No	Always	
fullnameOverride	Label to override name of api-gateway micro-service name	Yes	ingress	
serviceMeshCheck	Load balancing will be handled by Ingress gateway, if true it would be handled by serviceMesh	Yes	false	

Table 3-5 (Cont.) Fixed value parameters

Parameter	Description	Mandatory Parameters	Dafault Value	Notes
cipherSuites	Supported Cipher Suites in Ingress	No	- 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	
cncoamGatewayEnable	CnCoam Gateway Enabled	No	false	Change it to true if required
maxConnectionsQueuedPerDestination	Jetty Client Settings	No	4096	

Table 3-5 (Cont.) Fixed value parameters

Parameter	Description	Mandatory Parameters	Dafault Value	Notes
maxConnectionsPerDestination	Jetty Client Settings	No	12 (This will be used when serviceMeshCheck is enabled)	
maxConnectionsPerIp	Jetty Client Settings	No	12	
connectionTimeout	Jetty Client Settings	No	10000	

Table 3-6 Global Parameters: Egress Gateway

Parameter	Description	Mandatory Parameters	Dafault Value	Notes
global.appinfoServiceEnable	Enabled to get RBAC permission for k8s apiserver communication	Yes	true	
global.dockerRegistry	Name of the Docker registry which hosts Egress docker images.	Yes	reg-1:5000	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		No	8080	
serviceEgressGateway.sslPort	SSL Port	No	8442	
serviceEgressGateway.actuatorPort	Actuator Port	No	9090	
enableOutgoingHttps	Enabling it for outgoing https request	No	false	Change it to true for enabling https for outgoing requests.
K8ServiceCheck	Enable this if loadbalancing is to be done by egress instead of K8s	No	false	
scpHttpHost	Scp HTTP IP/FQDN	Yes	NA	
scpHttpPort	Scp PORT	Yes	NA	

Table 3-6 (Cont.) Global Parameters: Egress Gateway

Parameter	Description	Mandatory Parameters	Dafault Value	Notes
scpHttpsHost	Scp HTTPS IP/FQDN	Yes	NA	
scpHttpsPort	Scp HTTPS PORT	Yes	NA	
scpApiPrefix	Change this value to corresponding prefix "/" 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.
scpDefaultScheme	Default scheme applicable when 3gpp-sbi-target-apiroot header is missing	No	https	
scpIntegrationEnabled	Change this to false when scp integration is not required	No	true	
headlessServiceEnabled	Enabling this will make the service type default to ClusterIP	No	false	

Table 3-6 (Cont.) Global Parameters: Egress Gateway

Parameter	Description	Mandatory Parameters	Dafault Value	Notes
cipherSuites	Supported Cipher Suites in Egress	No	- 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	Connection with other ciphers would be rejected.
log.level	Log level	No	DEBUG	
jaegerTracingEnabled	Enable jaeger tracing	No	false	Change it to true if needed.

Table 3-6 (Cont.) Global Parameters: Egress Gateway

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

Table 3-6 (Cont.) Global Parameters: Egress Gateway

Parameter	Description	Mandatory Parameters	Dafault Value	Notes
consumerPlmnMNC	MNC of service Consumer.	No	Modify the field with actual value , required if oAuth is enabled.	
consumerPlmnMCC	MCC of service Consumer.	No	Modify the field with actual value , required if oAuth is enabled.	
maxConnectionsQueuedPerDestination	jetty client configuration	No	1024	
maxConnectionsPerDestination		No	4	
maxConnectionsPerIp	Max Connections allowed per Ip	No	4	
connectionTimeout	Connection timeout in milli seconds	No	1000	
egressGwCertReloadEnabled		No	true	

Table 3-7 Service Customizable Parameters

Parameter	Description	Mandatory Parameters	Dafault Value	Notes
type	type of service	Yes	ClusterIP	Possible values are :- ClusterIP, NodePort, LoadBalancer and ExternalName

Table 3-7 (Cont.) Service Customizable Parameters

Parameter	Description	Mandatory Parameters	Dafault Value	Notes
ssl.privateKey.k8SecretName	Name of the privatekey secret	Yes (If enableOutgoingHttps is true otherwise No)	n/a	
ssl.privateKey.k8NameSpace	Namespace of privatekey	Yes (If enableOutgoingHttps is true otherwise No)	n/a	
ssl.privateKey.rsa.fileName	rsa private key file name	Yes (If enableOutgoingHttps is true otherwise No)	n/a	
ssl.privateKey.ecdsa.fileName	ecdsa private key file name	Yes (If enableOutgoingHttps is true otherwise No)	n/a	
ssl.certificate.k8SecretName	Name of the privatekey secret	Yes (If enableOutgoingHttps is true otherwise No)	n/a	
ssl.certificate.k8NameSpace	Namespace of privatekey	Yes (If enableOutgoingHttps is true otherwise No)	n/a	
ssl.certificate.rsa.fileName	rsa private key file name	Yes (If enableOutgoingHttps is true otherwise No)	n/a	
ssl.certificate.ecdsa.fileName	ecdsa private key file name	Yes (If enableOutgoingHttps is true otherwise No)	n/a	

Table 3-7 (Cont.) Service Customizable Parameters

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

Table 3-7 (Cont.) Service Customizable Parameters

Parameter	Description	Mandatory Parameters	Dafault Value	Notes
ssl.trustStorePassword.fileName	File name that has password for trustStore	Yes (If enableOutgoingHttps is true otherwise No)	n/a	

Table 3-8 Resource Customizable Parameters

Parameter	Description	Mandatory Parameters	Dafault Value	Notes
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	

Table 3-8 (Cont.) Resource Customizable Parameters

Parameter	Description	Mandatory Parameters	Dafault Value	Notes
minReplicas	Minimum replicas to scale to maintain an average CPU utilizati		2	
maxReplicas	Maximum replicas to scale to maintain an average CPU utilization		5	

Table 3-9 Routes Config Customizable Parameters

Parameter	Description	Mandatory Parameters	Dafault Value	Notes
id	id of the route	Yes (If scpintegrationenabled is true)		Can be any name of your choice
uri	Provide any dummy url , existing url can also left with existing value	Yes (If scpintegrationenabled is true)		Please note provided sample url does not make any impact (http or https) as url's will be constructed in the code.
path	Provide the path to be matched.	Yes (If scpintegrationenabled is true)		
order	Provide the order of the execution of this route.	Yes (If scpintegrationenabled is true)		
filterName	Provide filtername as "ScpFilter"	Yes (If scpintegrationenabled is true)		

Table 3-10 Fixed value parameters

Parameter	Description	Mandatory Parameters	Dafault Value	Notes
erviceEgressGateway.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.

Table 3-10 (Cont.) Fixed value parameters

Parameter	Description	Mandatory Parameters	Dafault Value	Notes
deployment EgressGateway.image	Image name of egress gateway	No	ocegress_gateway	
deployment EgressGateway.imageTag	Image Tag name of egress gateway	No	1.6.1	
deployment EgressGateway.pullPolicy	Pull Policy of Image	No	Always	
initContainersImage.name	Image name of initContainer	No	configurationinit	
initContainersImage.tag	Image tag name of initContainer	No	1.1.1	
initContainersImage.pullPolicy	Pull Policy of Image	No	Always	
updateContainersImage.name	Image name of updateContainer	No	configurationupdate	
updateContainersImage.tag	Image tag name of updateContainer	No	1.1.1	
updateContainersImage.pullPolicy	Pull Policy of Image	No	Always	
fullnameOverride		Yes	egress	
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	
jaegerTracingEnabled	JaegerTracing Enabled	No	false	
ssl.tlsVersion	TLS Version	Yes	TLSv1.2	
initialAlgorithm		Yes	RSA256	ES256 can also be used, but corresponding certificates need to be used.

Table 3-11 N32-Forward Internetwork Packet Exchange (`n32f-ipx`)

Parameter	Description	Mandatory Parameters	Dafault Value	Notes
replicaCount	Number of replicas initiall	yes	1	
log.level	Describes log level	no	INFO	
resources.limit.cpu	Resource Requirements(limit of cpu)	Yes	4	
resources.limit.memory	Resource Requirements(limit of memory)	Yes	4	
resources.requests.cpu	Resource Requirements(requested cpu)	Yes	4	
resources.requests.cpu	Resource Requirements(requested memory)	Yes	4	
resources.target.averageCpuUtil	Resource Requirements(avg cpu utilisation)	Yes	50	
configs.secretName	Name of the secret containing Private Key used by signing the JSON Patch Document created by IPX	Yes	ocsepp-ipx-secret	
configs.namespace	Namespace of the secret	Yes	seppsvc	
configs.algorithm	Algorithm used for signing JSON Patch Document	Yes	ES256	
configs.keyName	Private Key Name in the secret	Yes	private_key.pem	
configs.kid	Kid used for signing JSON Patch Document	Yes	1234	
configs.ipxIdentity	IPX Idenity	Yes	ipx.oracle.com	
configs.jaegerTracingEnabled	Enables Jaeger Tracing	Yes	false	
configs.openTracing.jaeger.udpSender.host	Jaeger Tracing Host	Yes(if jaeger is enabled)	jaeger-agent.cne-infra	
configs.openTracing.jaeger.udpSender.port	Jaegar Tracing Port	Yes(if jaeger is enabled)	6831	
configs.openTracing.jaeger.logSpans	Jaegar Tracing Logs	Yes(if jaeger is enabled)	false	
configs.openTracing.jaeger.probabilisticSamplingRate	Jaegar Tracing Sampling Rate	Yes(if jaeger is enabled)	0.5	

Table 3-11 (Cont.) N32-Forward Internetwork Packet Exchange (`n32f-ipx`)

Parameter	Description	Mandatory Parameters	Dafault Value	Notes
maxConnectionsQueuedPerDestination	jettyClient Config	No	4096	
maxConnectionsPerDestination	Max Connections allowed per destination	No	12	
maxConnectionsPerIp	Max Connections allowed per Ip	No	12	
connectionTimeout	Connection timeout in millsec	No	10000	

Table 3-12 JSON Web Signature Service (`jws-svc`)

Parameter	Description	Mandatory Parameters	Dafault Value	Notes
replicaCount	Number of replicas for the pod	yes	1	
minReplicas	Minimum Number of Relicas	yes	1	
maxReplicas	Maximum num of replicas of pod	yes	3	
resources.limit.cpu	Resource Requirements(limit of cpu)	Yes	4	
resources.limit.memory	Resource Requirements(limit of memory)	Yes	4	
resources.requests.cpu	Resource Requirements(requested cpu)	Yes	4	
resources.requests.cpu	Resource Requirements(requested memory)	Yes	4	
resources.target.averageCpuUtil	Resource Requirements(avg cpu utilisation)	Yes	50	
log.level	Log Lovel	yes	INFO	
configs.jaegerTracingEnabled	Enables Jaeger Tracing	Yes	false	
configs.openTracing.jaeger.udpSender.host	Jaeger Tracing Host	Yes(if jaeger is enabled)	jaeger-agent.cne-infra	
configs.openTracing.jaeger.udpSender.port	Jaegar Tracing Port	Yes(if jaeger is enabled)	6831	
configs.openTracing.jaeger.logSpans	Jaegar Tracing Logs	Yes(if jaeger is enabled)	false	

Table 3-12 (Cont.) JSON Web Signature Service (`jws-svc`)

Parameter	Description	Mandatory Parameters	Dafault Value	Notes
configs.openTracing.jaeger.probabilisticSamplingRate	Jaegar Tracing Sampling Rate	Yes(if jaeger is enabled)	0.5	

4
Upgrading SEPP

This section includes information about upgrading an existing SEPP deployment.

When you attempt to upgrade an existing SEPP deployment, the running set of containers and pods are replaced with the new set of containers and pods. However, If there is no change in the pod configuration, the running set of containers and pods are not replaced.

If you need to change any configuration then change the `ocsepp-custom-values-1.3.0.yaml` file with new values.

> **Note:**
>
> It is advisable to create a backup of the file before changing any configuration.

> **Caution:**
>
> Upgrading SEPP within same release supports only configuration changes.

Execute the following command to upgrade an existing SEPP deployment:

```
$ helm upgrade <release> <helm chart> [--version <OCSEPP version>] -f
      <ocsepp_customized_values.yaml>
```

For example:

```
$ helm upgrade <release> <helm chart> [--version <OCSEPP version>] -f
ocsepp-custom-values-1.3.0.yaml
```

To check the status of the upgrade, execute:

```
helm status <helm-release>
```

For example: `helm status ocsepp`

Table 4-1 Parameters and Definitions during SEPP Upgrade

Parameters	Definitions
`<helm chart>`	It is the name of the chart that is of the form `<repository/ocsepp>`. For example: `reg-1/ocsepp or cne-repo/ocsepp`
`<release>`	It can be found in the output of `helm list` command

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>`

5
Uninstall SEPP

Following is the procedure to uninstall SEPP:

1. Execute command to uninstall SEPP deployment:

   ```
   helm del --purge <helm_release>
   ```

   Example:

   ```
   helm del --purge ocsepp
   ```

2. Execute the following command to delete kubernetes namespace :

   ```
   kubectl delete namespace <sepp_namespace>
   ```

   Example:

   ```
   kubectl delete namespace seppsvc
   ```