R6 - Installation Documentation of Enterprise Applications on Lightweight 5G Telco Edge (EALTEdge)

- Introduction
- How to use this document
- Deployment Architecture
- Pre-Installation Requirements
  - Hardware Requirements
    - Minimum Hardware Requirements
    - Recommended Hardware Requirements
  - Software Prerequisites
  - Database Prerequisites
    - Schema scripts
  - Other Installation Requirements
    - Jump Host Requirements
    - Network Requirements
    - Bare Metal Node Requirements
    - Execution Requirements (Bare Metal Only)
- Installation High-Level Overview
  - EALTEdge Installation Mode:
    - AIO(All in One) mode:
    - MUNO(Multi Node) Mode:
  - Bare Metal Deployment Guide
    - Install Bare Metal Jump Host
    - Creating a Node Inventory File
    - Creating the Settings Files
    - Running
  - Virtual Deployment Guide
    - Standard Deployment Overview
      - Jump Host Software Installations:
      - Jump Host Pre-Configurations for Center Components Installation
      - Installing Mode : EALTEdge using Ansible-Playbooks
    - Snapshot Deployment Overview
    - Special Requirements for Virtual Deployments
    - Install Jump Host
    - Verifying the Setup - VM's
  - Upstream Deployment Guide
    - Upstream Deployment Key Features
    - Special Requirements for Upstream Deployments
    - Scenarios and Deploy Settings for Upstream Deployments
    - Including Upstream Patches with Deployment
    - Running
    - Interacting with Containerized Overcloud
- Verifying the Setup
  - Verifying EALTEdge Deployment
  - Deploy Application in EALTEdge
- Developer Guide and Troubleshooting
  - Uninstall Guide
    - Using Ansible Playbooks
    - Vault documentation
- Troubleshooting
- Maintenance
  - Blueprint Package Maintenance
    - Software maintenance
    - Hardware maintenance
  - Blueprint Deployment Maintenance
- Frequently Asked Questions
- License
- References
- Definitions, acronyms and abbreviations

Introduction

The guide covers the installation details which are related to Enterprise Applications on Lightweight 5G Telco Edge (EALTEdge) Blueprint.

This guide covers detailed information of the various types of deployments, detailed steps and what are the various components it will install. In addition, the guide provides information on hardware requirements, prerequisite software and minimum hardware requirements. On successful deployment, Center and Edge Nodes will be installed. The number of nodes in Center cluster and Edge node in the cluster is configurable.

The CENTER Node is a K8s Cluster and EDGE Node is a K8s Cluster.

How to use this document

The document includes details of prerequisites /pre-installation, installation and uninstalls steps.

The prerequisites and pre-installation software and hardware should be ready before executing the installation steps.

In BP first release Two types of installation mechanisms are provided, as below

1. Ansible-Playbook single command
2. Command Line Interface (CLI)

Deployment Architecture

The Deployment Architecture consists of the following nodes

- One-Click Deployment Node
- Center Node
- Edge Node

Note: For Development environment two nodes is sufficient, where one node plays a dual role of One-Click Deployment Node and MECM Node with other as MEC Host.

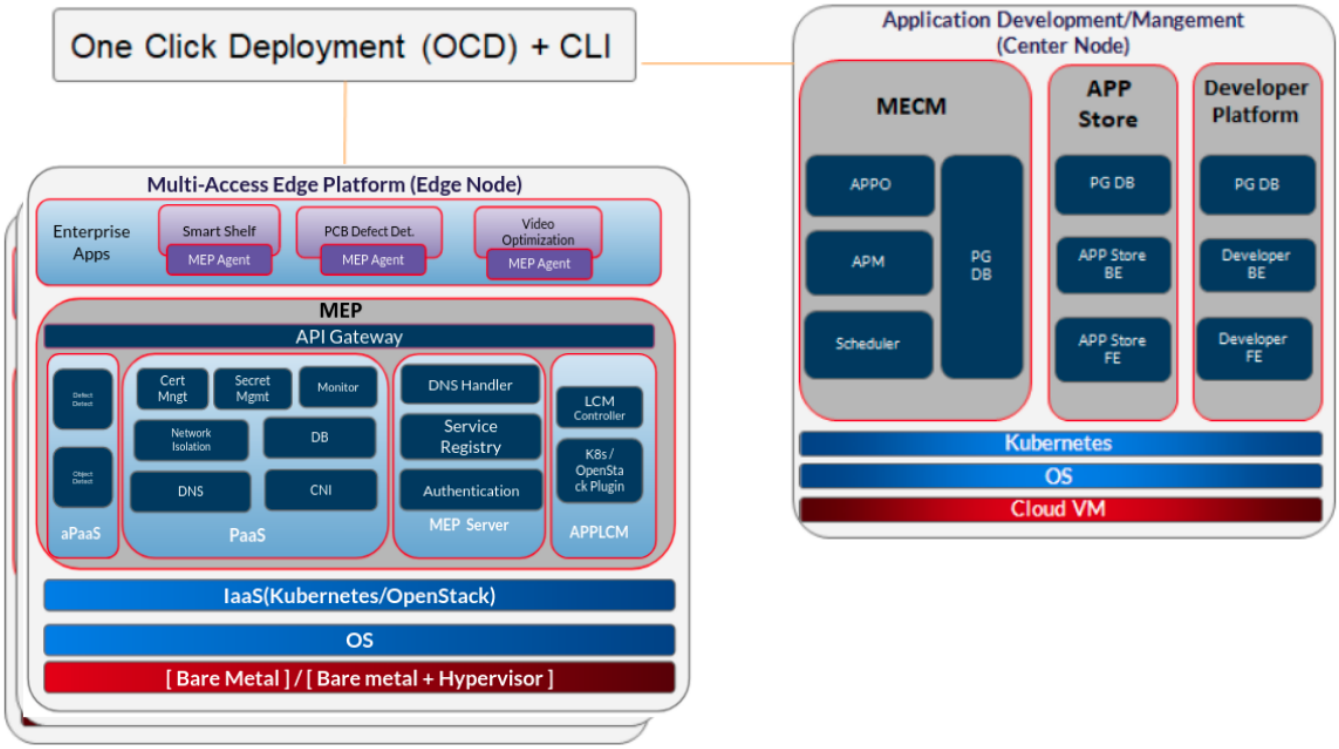


Figure: EALTEdge Deployment Architecture

***Note:** EALTEdge Blueprint Deployment has been tested on Cloud VM and is not tested on Bare-Metal Environment. Though, theoretically deployment should work in bare metal, provided hardware and software prerequisites are met. Kindly refer R6 - Test Documentation of Enterprise Applications on Lightweight 5G Telco Edge (EALTEdge) to get details on the tested deployment.*

Pre-Installation Requirements

Hardware Requirements

The number of Hardware requirements depends mainly on the Use Case Scenario and the enterprise scale. A use case can have one MECM Cluster with one or multiple MEC Host clusters.

The minimum number of logical nodes(all 3 nodes can be depployed on single VM or on multiple VMs) required for a complete EALTEdge Topology is three. (Bare-Metal or Virtual Machines)

1) Deployment Node

2) Center Node

3) Edge Node

Note: The Hardware details provided are of Virtual Machine configurations.

Minimum Hardware Requirements

CENTER Node	
HW Aspect	Requirements
# of Node(s)	A virtual machine hosted in any Cloud Provider having internet connectivity.
# of CPU	8
Architecture	x86_AMD64 or ARM64.
RAM	8 GB
Disk	120 GB ~ 512GB
Networks	1

EDGE Node(s)	
HW Aspect	Requirements
# of Node(s)	1 MEC Host
# of CPU	4
Architecture	x86_AMD64 or ARM64.
RAM	4 GB
Disk	20 GB ~ 256 GB
Network	1

Note: The above specifications are given considering the EALTEdge CI / CD environment. User can try lower configuration considering lightweight components being used.

Recommended Hardware Requirements

CENTER Node	
HW Aspect	Requirements
# of Node(s)	A virtual machine hosted in any Cloud Provider having internet connectivity.
# of CPU	8
Architecture	x86_AMD64 or ARM64.
RAM	8 GB
Disk	120 GB ~ 512GB
Networks	1

EDGE Node(s)	
HW Aspect	Requirements
# of Node(s)	1 MEC Host
# of CPU	4
Architecture	x86_AMD64 or ARM64.

RAM	4 GB
Disk	20 GB ~ 256 GB
Network	1

Software Prerequisites

- Virtual Machines preinstalled with Ubuntu 18.04 for MECM Node.
- Virtual Machines preinstalled with Ubuntu 18.04 for MEC Host Nodes
- root user created in the Deployment Node, MEC Node and MEC Host Node.
- SSH Server running in all the Nodes.
- Ansible > 2.10.7 installed in One Click Deployment Node (Jump Host)
- git installed in Jump Host.

Database Prerequisites

Schema scripts

N/A

Other Installation Requirements

Jump Host Requirements

Network Requirements

- Internet connectivity in OCD Host, CENTER and EDGE Nodes.
- The CENTER Node and EDGE Node should be able to ping each other.

Bare Metal Node Requirements

N/A

Execution Requirements (Bare Metal Only)

N/A

Installation High-Level Overview

The blueprint provides one click deployment for installing the EALTEdge blueprint components.

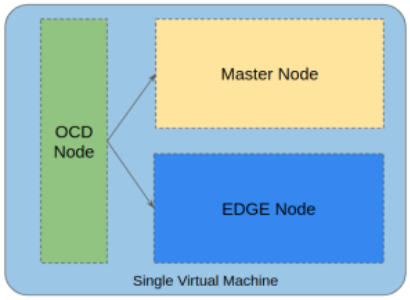
EALTEdge Installation Mode:

EALTEdge supports 2 Mode of installation: Multi Node and All-In-One (AIO) Node deployment.

AIO(All in One) mode:

In this mode, all 3 nodes (OCD which is deployment node, Center node and Edge node) are deployed on single VM.

The logical deployment topology can be seen here.

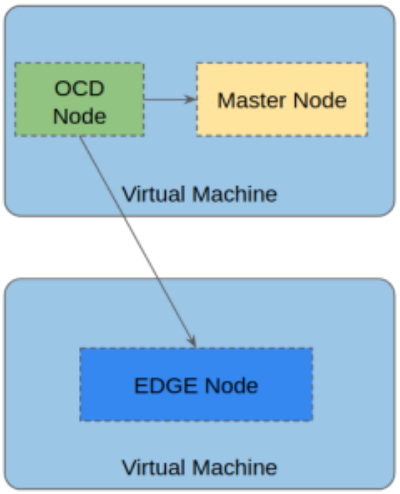


MUNO(Multi Node) Mode:

In this mode, all 3 nodes (OCD which is deployment node, Center node and Edge node) can be deployed on multiple VM.

This mode can have a OCD node deployed on a VM, Center node deployed on same OCD VM or on different VM and EDGE node deployed on different VM.

The logical deployment topology can be seen here.



Bare Metal Deployment Guide

Install Bare Metal Jump Host

Note: EALTEdge Blueprint Deployment has been tested on Huawei Cloud Virtual Machines and is not tested on Bare-Metal Environment.

Though theoretically deployment should run successfully in bare metal too provided hardware and software prerequisites are met.

Creating a Node Inventory File

N/A

Creating the Settings Files

N/A

Running

N/A

Virtual Deployment Guide

For Virtual Deployment minimum **2** Virtual machines(OCD and Center node can be deploy on same VM or in different VMs), following are the virtual machines and their usage

No	Usage
1	One Click Deployment Node
2	CENTER Node
3	EDGE Node

All the nodes should have internet connectivity , network interface and network connectivity between the VM's.

Standard Deployment Overview

Jump Host Software Installations:

Login to the Jump Host and perform the below steps:

1. Install Ansible > 2.10.7 [https://docs.ansible.com/ansible/latest/installation_guide/intro_installation.html]
2. Install git
3. Install python3 and pip3

Jump Host Pre-Configurations for Center Components Installation

Login to the Jump Host and perform the below configuration steps (Steps : as below-

1. Generate public key :

ssh-keygen -t rsa

2. Setup password-less login -

- If you get authentication issue you can change the permission

Open file: vi /etc/ssh/sshd_config

- PermitRootLogin yes

- PasswordAuthentication yes

Restart ssh service:

- sudo systemctl restart ssh.service

For EdgeGallery AIO mode:

Login from ocd to center and ocd to edge in a single node.

- sshpass -p <password> ssh-copy-id -p <ssh-port> -o StrictHostKeyChecking=no root@<node_ip>

For EdgeGallery Muno mode:

Login from ocd to center in a controller node

- sshpass -p <password> ssh-copy-id -p <ssh-port> -o StrictHostKeyChecking=no root@<controller-node_ip>
- sshpass -p <password> ssh-copy-id -p <ssh-port> -o StrictHostKeyChecking=no root@<edge-node_ip>

Login from ocd to edge in a edge node

- sshpass -p <password> ssh-copy-id -p <ssh-port> -o StrictHostKeyChecking=no root@<controller-node_ip>
- sshpass -p <password> ssh-copy-id -p <ssh-port> -o StrictHostKeyChecking=no root@<edge-node_ip>

3. These command are require in both AIO and MUNO(Controller and Edge Node) mode.

cp -p /etc/passwd /etc/passwd.bkp

cp -p /etc/group /etc/group.bkp

id ubuntu

groupmod -g 600 ubuntu

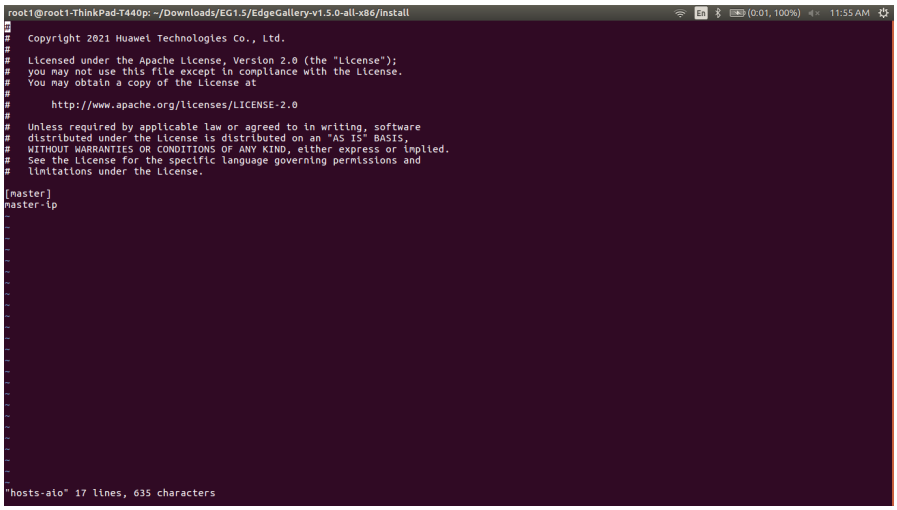
id ubuntu

4. Review and Change Parameters

For EdgeGallery AIO Mode:

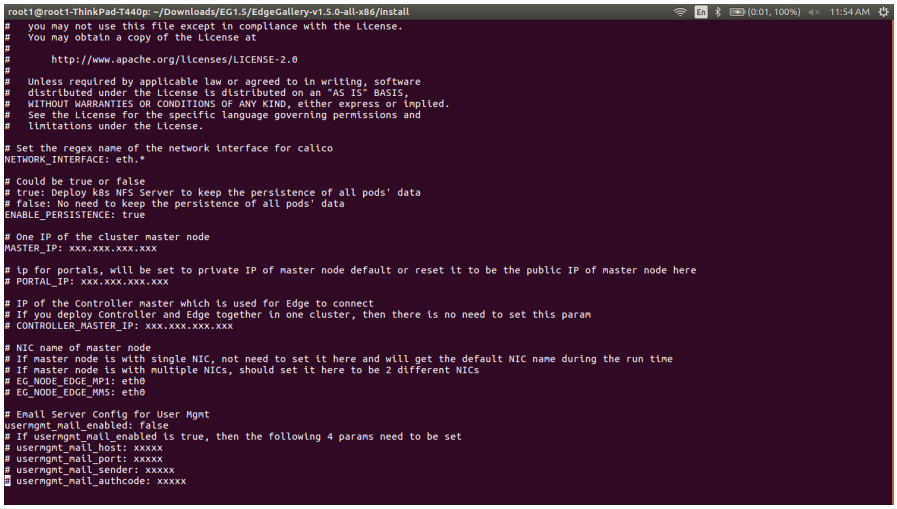
ealt-edge/ocd/infra/playbooks/hosts-aio

- *Here user can use the private IP of a node*



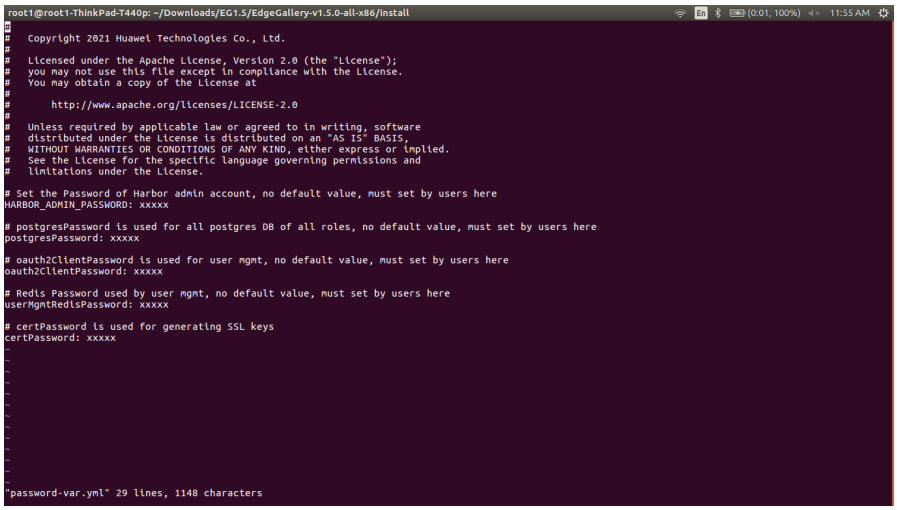
ealt-edge/ocd/infra/playbooks/var.yml

- *NETWORK_INTERFACE: regex for network interface on the VM. (user can be check ineterrface name by ifconfig and provide inerface name accordingly for example like eth.*)*
- *MASTER_IP: Here user can use the private IP of a node*
- *PORTAL_IP: If portal need to be access over internet then uncomment the PORTAL_IP and use public IP as a PORTAL_IP otherwise portal will be accessible only on private IP default.*



ealt-edge/ocd/infra/playbooks/password-var.yml

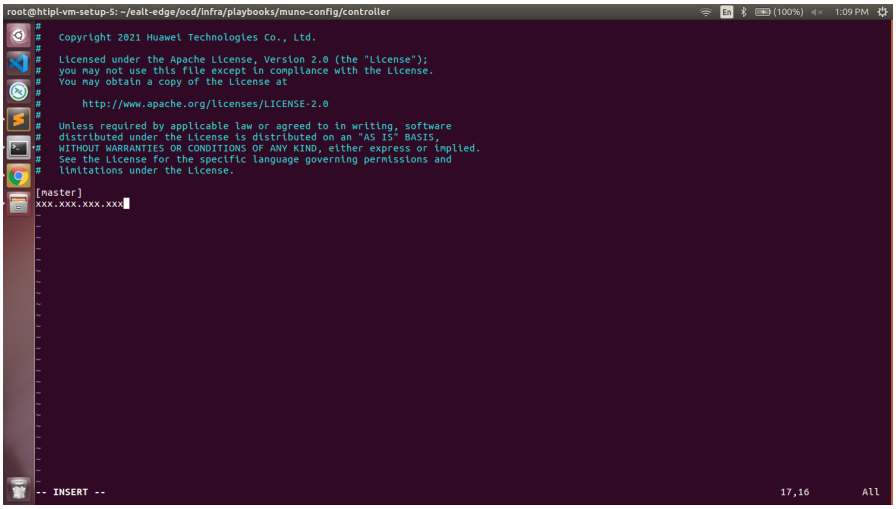
- All passwords must include capital letters, lowercase letters, numbers and special characters and whose length must be no less than 8 characters. Also there should be no special characters & in it. Otherwise, the deployment will failed because of these simple passwords.
- A sample password could be "Harbor@12345"



For EdgeGallery MUNO Mode:

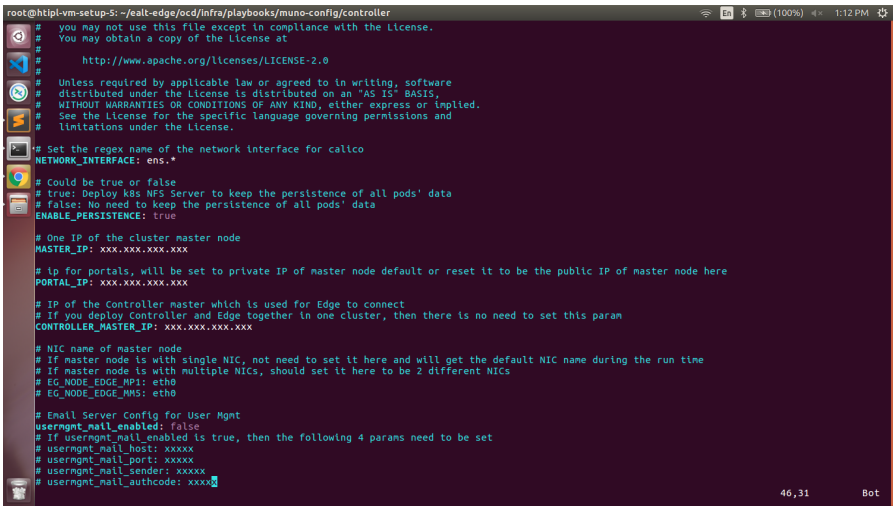
ealt-edge/ocd/infra/playbooks/muno-config/controller/hosts-muno-controller

- *Here user can use the private IP as a master IP of a Controller node*



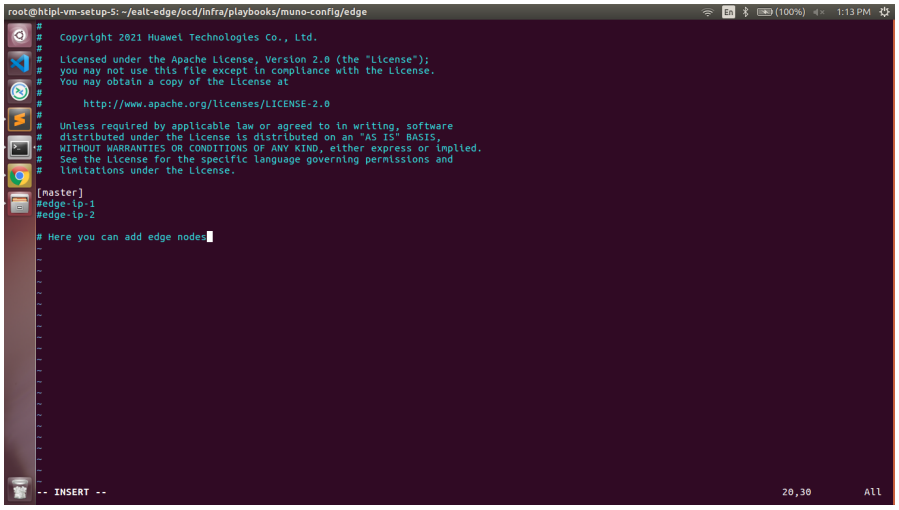
ealt-edge/ocd/infra/playbooks/muno-config/controller/var.yml

- *NETWORK_INTERFACE: regex for network interface on the VM. (user can be check ineterrface name by ifconfig and provide inerface name accordingly for example like eth.*)*
- *MASTER_IP: Here user can use the private IP of a controller node*
- *PORTAL_IP: If portal need to be access over internet then uncomment the PORTAL_IP and use public IP of a controller node as a PORTAL_IP otherwise portal will be accessible only on private IP default.*
- *CONTROLLER_MASTER_IP: Private IP of the Controller node.*



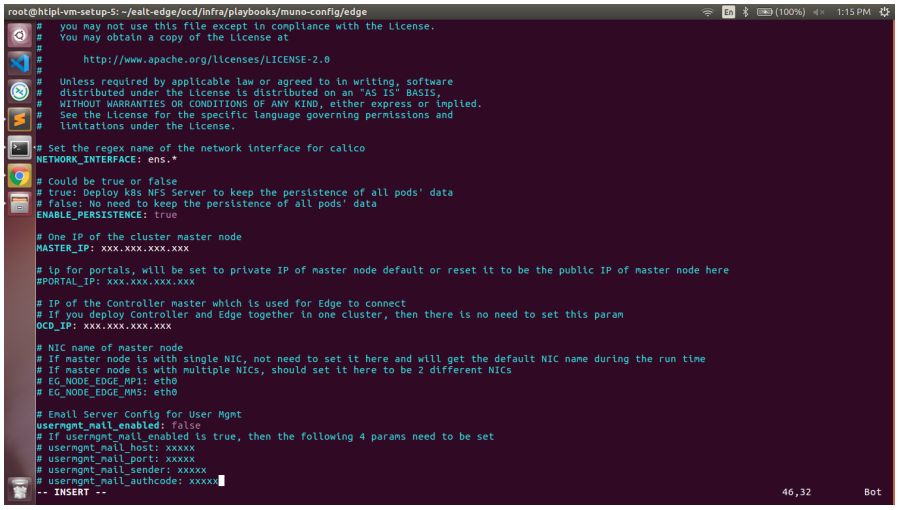
ealt-edge/ocd/infra/playbooks/muno-config/edge/hosts-muno-edge

- *Here user can use the private IP as a master IP of a Edge node*



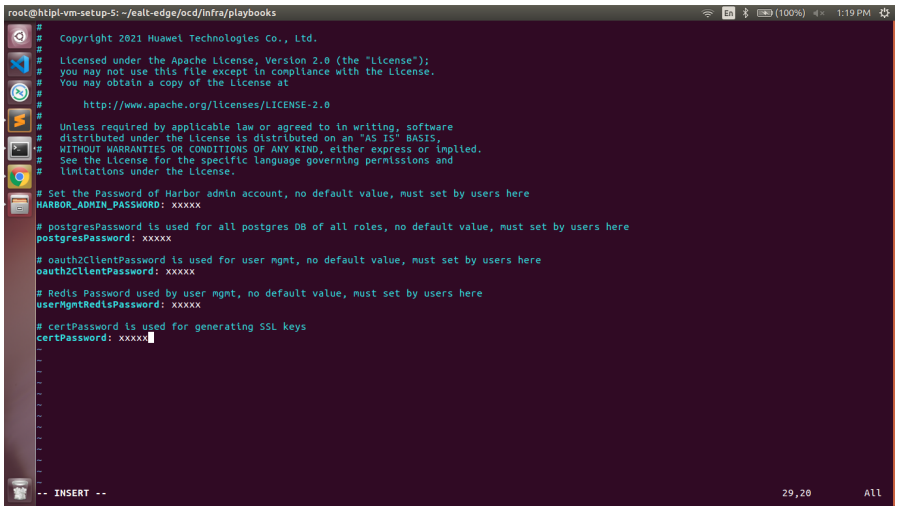
ealt-edge/ocd/infra/playbooks/muno-config/edge/var.yml

- *NETWORK_INTERFACE: regex for network interface on the VM. (user can be check ineterrface name by ifconfig and provide inerface name accordingly for example like eth.*)*
- *MASTER_IP: Here user can use the private IP of a edge node*
- *OCD_IP: Here user can use the private IP of a Controller Node which is used for Edge to connect*



ealt-edge/ocd/infra/playbooks/password-var.yml

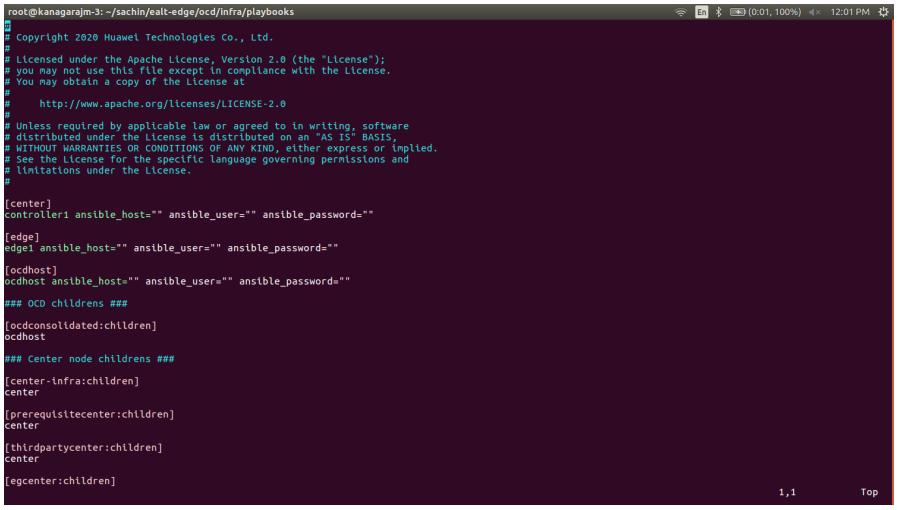
- All passwords must include capital letters, lowercase letters, numbers and special characters and whose length must be no less than 8 characters. Also there should be no special characters & in it. Otherwise, the deployment will failed because of these simple passwords.
- A sample password could be "Harbor@12345"



For EALT-EDGE stack:

ealt-edge/ocd/infra/playbooks/ealt-inventory.ini

* Here user can put the public IP in center, edge, ocdhost node.



Installing Mode : EALTEdge using Ansible-Playbooks

1. git clone the ealt-edge repo, to download the software to install the EALTEdge Environment.

root@akraino-mec-0001:~# git clone "https://gerrit.akraino.org/r/ealt-edge"

2. go to the below directory

root@akraino-mec-0001:~# cd ealt-edge/ocd/infra/playbooks

3. Modify the Configuration File :

ealt-inventory.ini with the details of CENTER and EDGE Nodes.

For Edge Gallery installation:

MUNO-Mode:

Execute the below command:

cd ealt-edge/ocd/infra/playbooks

ansible-playbook -i muno-config/controller/hosts-muno-controller ealt-eg-muno-controller.yml --extra-vars "operation=install" -e "ansible_user=root"

ansible-playbook -i muno-config/edge/hosts-muno-edge ealt-eg-muno-edge.yml --extra-vars "operation=install" -e "ansible_user=root"

For AIO mode:

Execute the below command

cd ealt-edge/ocd/infra/playbooks

ansible-playbook ealt-eg-aio-latest.yml -i hosts-aio --extra-vars "operation=install" -e "ansible_user=root"

Installation of ealt-edge stack:

ansible-playbook ealt-all.yml -i ealt-inventory.ini --extra-vars "operation=install"

Once the execution is completed in console will see prompt "EALTEdge Environment Installed , Components Install CENTER and EDGE Nodes Successfully"

Snapshot Deployment Overview

N/A

Special Requirements for Virtual Deployments

N/A

Install Jump Host

N/A

Verifying the Setup - VM's

N/A

Upstream Deployment Guide

Upstream Deployment Key Features

N/A

Special Requirements for Upstream Deployments

N/A

Scenarios and Deploy Settings for Upstream Deployments

N/A

Including Upstream Patches with Deployment

N/A

Running

N/A

Interacting with Containerized Overcloud

N/A

Verifying the Setup

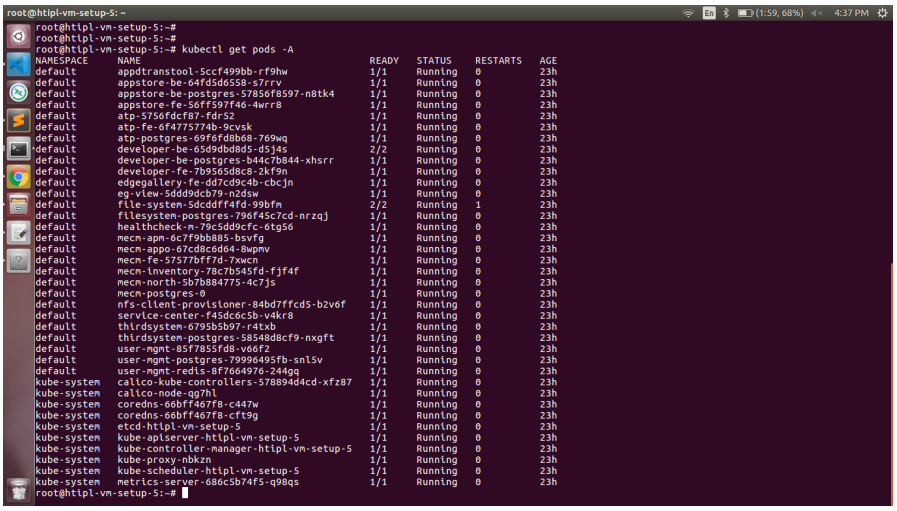
Verifying EALTEdge Deployment

Currently the verification is manually done.

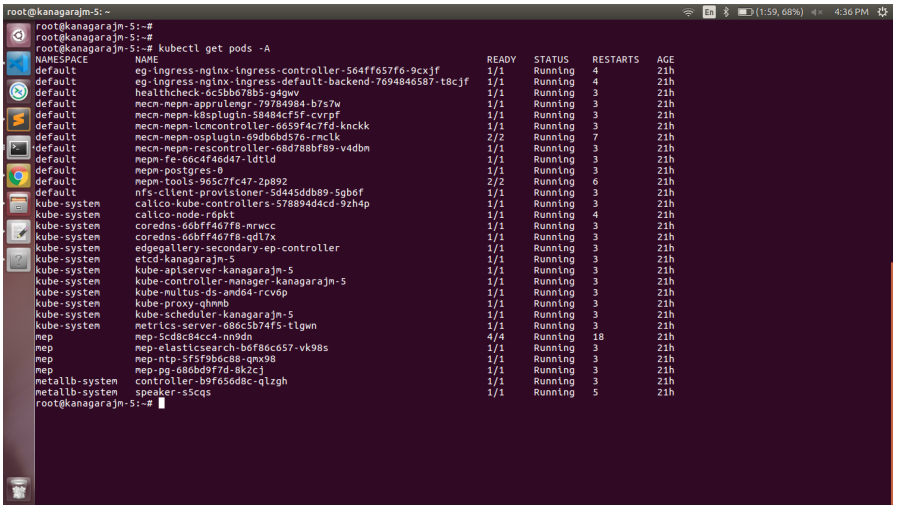
In muno mode

1- Login to the Center Node and check whether K8S cluster is installed.

Components and Services running in Controller Node



Components and Services running EDGE Node



Deploy Application in EALTEdge

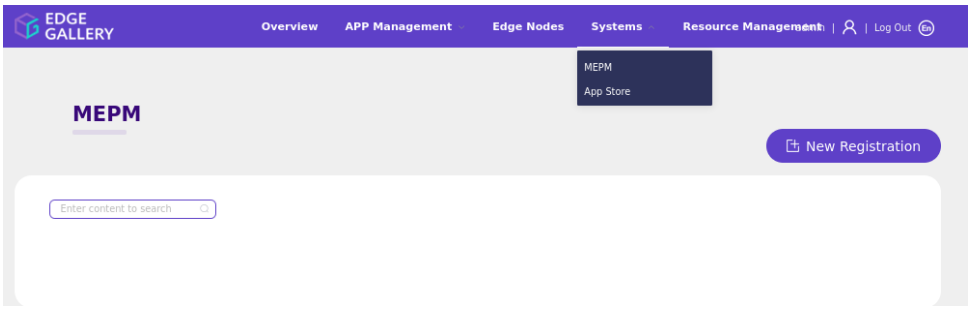
1. Login to MECM Portal https://ip:30093

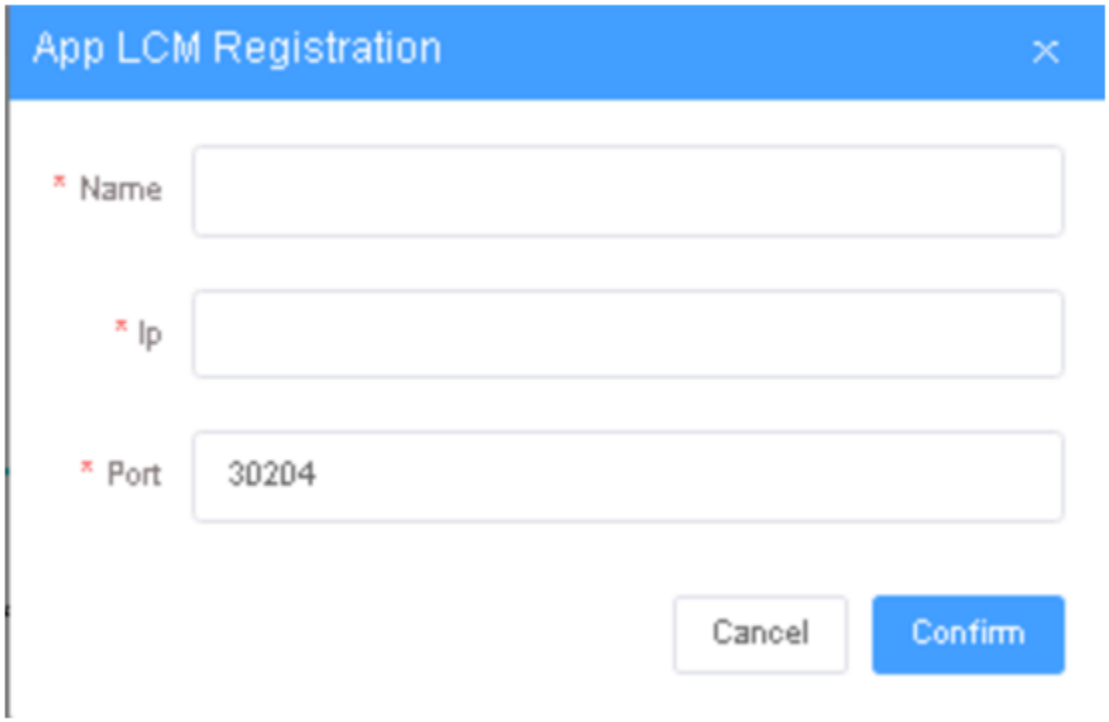
   1.1 click on **Systems ->App LCM ->New Registration**

   Name: Applcm(any general name)

   IP: applcm"public ip"

   Port: 30204





1.2. click on **Systems ->App Store ->New Registration**

App Store Name: appstore(any general name)

IP: Appstore public ip

Port: 30099

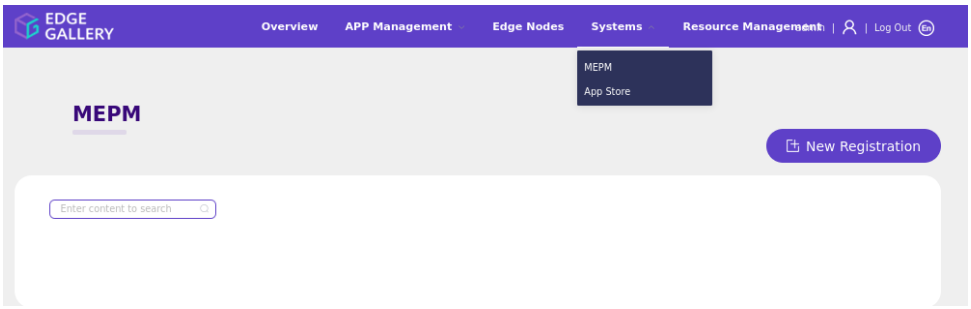
Appstore Repo: {HarborIP:443}(192.168.1.1:443)

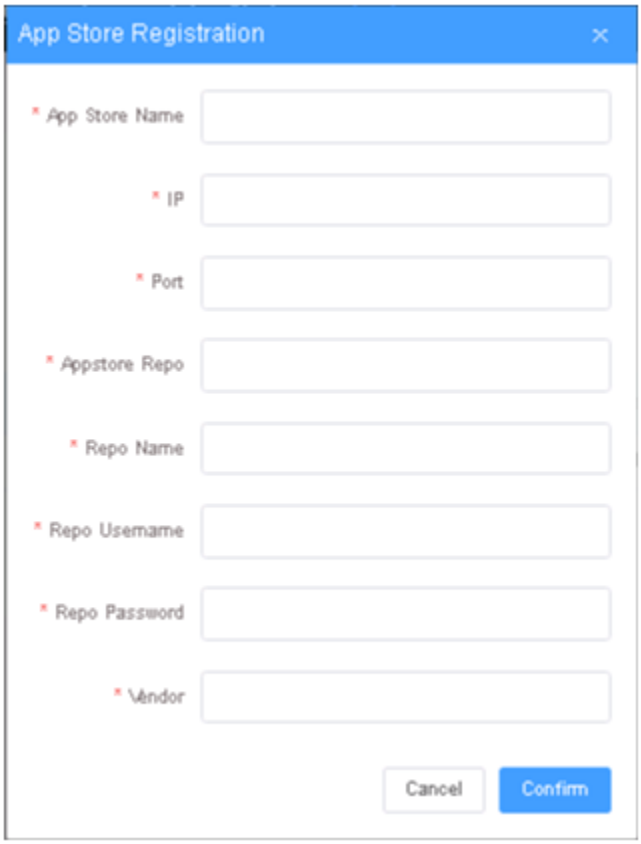
Repo Name: appstore(any general name)

Repo Username: admin(harbor user name)

Repo Password: Harbor@edge(harbor password)

Vendor: vendor(any general name)





2. log in to MECM Portal https://ip:30093

2.1. **Add k8s node:**

Click on **Edge Nodes ->New Rgistration**

System: k8s

Name: edge1(any general name)

IP: edge public IP

Location: Select from the drop-down

Architecture: x86

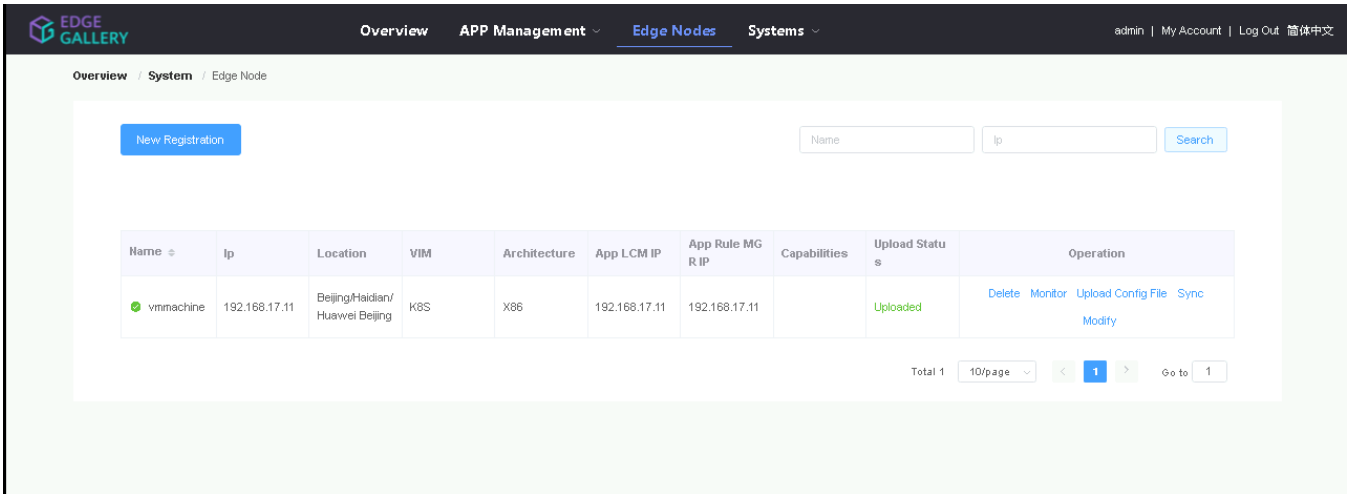
Capabilities: select none

App LCM: Select edge IP from the drop-down box

App Rule MGR: Select edge IP from the drop-down box

2.2. Download /root/.kube/config file from edge node

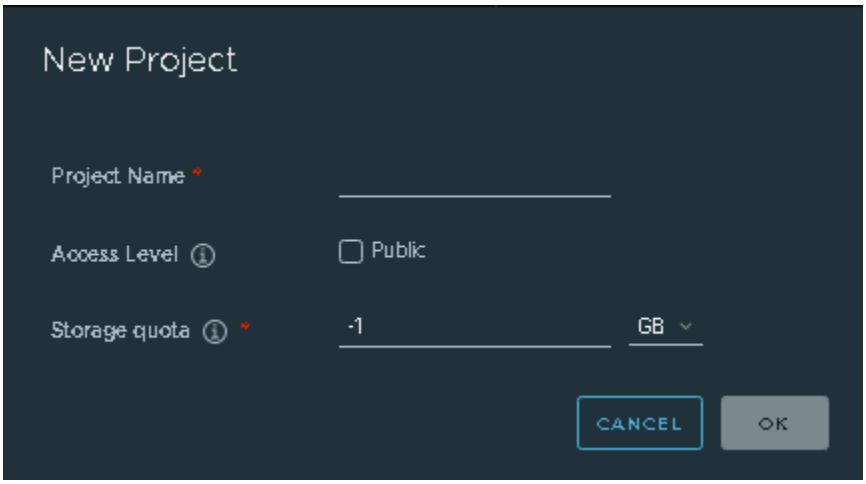
And click on **Upload config file** to upload.



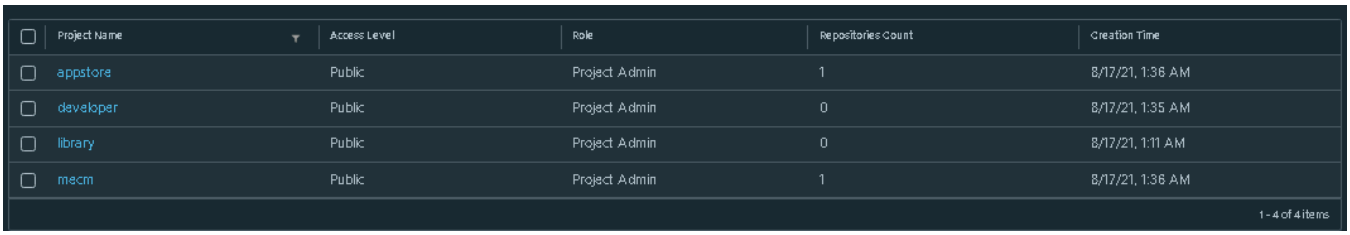
3. log in to harbor Portal https://ip:443

3.1. Add three **new projects**

3.2. Those three **projects' names** are appstore, developer, and mecm. And select **access level** to the public.



3.3. Final page will look like the below screenshot.



4. log in to Developer Portal https://ip:30092

4.1. Add sandbox env to deploy application before publishing

Click System ->Host Management ->Add Host

.

Name: general name

System: k8s

Lcmip: sandbox ip(for testing purpose can provide edge ip, if no sandbox env)

mecHost: sandbox ip(for testing purpose can provide edge ip, if no sandbox env)

Port: 30204

Protocol: https

Architecture: X86

Status: Normal

Port Range: leave as it is

Address: Bangalore

UploadConfig File: upload sandboxenvkubeconfig file

4.2 Demonstration of application Development & Deployment

Application Development
link - https://www.youtube.com/watch?v=AjQNG5d3p84&t=23s

Application Deployment
link - https://www.youtube.com/watch?v=PbxKpslVnmc&t=31s

Developer Guide and Troubleshooting

Uninstall Guide

Using Ansible Playbooks

For EALT-EDGE stack
root@akraino-mec-0001:~#ansible-playbook ealt-all-uninstall.yml -i ealt-inventory.ini --extra-vars "operation=uninstall"

For MUNO Mode

root@akraino-mec-0001:~#ansible-playbook -i muno-config/controller/hosts-muno-controller ealt-eg-muno-controller.yml --extra-vars "operation=uninstall" -e "ansible_user=root"

root@akraino-mec-0001:~#ansible-playbook -i muno-config/edge/hosts-muno-edge ealt-eg-muno-edge.yml --extra-vars "operation=uninstall" -e "ansible_user=root"

For AIO Mode

root@akraino-mec-0001:~#ansible-playbook -i hosts-aio ealt-eg-aio-latest.yml --extra-vars "operation=uninstall" -e "ansible_user=root"

Vault documentation

````
**This document explains how to generate certificate by using vault and cert manager**
##Cluster Architecture
![](Vault_Cert_Arch)
##Make a cluster
##The Image try to put with reference to our environment, with reference to EALT Edge. Can make a picture where
Vault will be running in MEC Host (as Root CA) , ##Cert Manager and Applications (App1, App2)
##1. Add helm repo
```
helm repo add hashicorp https://helm.releases.hashicorp.com
helm install vault hashicorp/vault
```
##2. Generate root token and Unseal Key
```
kubectl exec vault-0 -- vault operator init -key-shares=1 -key-threshold=1 -format=""
```
##Note: Root token we will use when we will login vault pod, Unseal Key and Root token will looks like below ex-
##Unseal Key 1: QcTX47IacKidIjFWSrkGLiQG1fwaqoInEz0SqAZ7rMs=
##Initial Root Token: s.A0SXgscZxbCeJRd1AjsVzvUU
````

##Generated Unseal key need to put in below command then vault will start running as a pod
```
kubectl exec -ti vault-0 -- vault operator unseal <Unseal Key>
```
##Vault is initialised as a pod
##By using below command can login in vault pod
```
kubectl exec -it vault-0 -- /bin/sh
```
##Vault Initialisation and Configuration Steps
####Once we initialize the vault pod we get unseal key and root token, need to put the root token
```
vault login <root token>
```
##Enable the PKI secrets engine
##By default, the secrets engine will mount at the name of the engine. To enable the secrets engine at a ##different path, use the -path argument.
```
vault secrets enable pki
```
##Keep the value in sync with the comment. 30 days, Increase the TTL by tuning the secrets engine. The default value of 30 days may be too short
```
vault secrets tune -default-lease-ttl=2160h -max-lease-ttl=87600h pki
```
##Configure a CA certificate and private key. It can generate ##its own self-signed root
ealtedge.com is a your common_name or base url
```
vault write pki/root/generate/internal common_name=ealtedge.com ttl=8760h
```
##Update the CRL location and issuing certificates. These values can be updated in the future.
```
vault write pki/config/urls issuing_certificates="http://127.0.0.1:8200/v1/pki/ca" crl_distribution_points="http://127.0.0.1:8200/v1/pki/crl"
```
##It will allow your domain and subdomain
```
vault write pki/roles/my-role allowed_domains=ealtedge.com allow_subdomains=true max_ttl=8760h
```
##Generate a new credential by writing to the /issue endpoint with the name of the role
##The output will include a dynamically generated private key and certificate which corresponds to the ##given role
##The issuing CA and trust chain is also returned for automation simplicity
```
vault write pki/issue/my-role common_name=www.ealtedge.com
```

####Enabling AppRole in Vault
```
vault auth enable approle
```

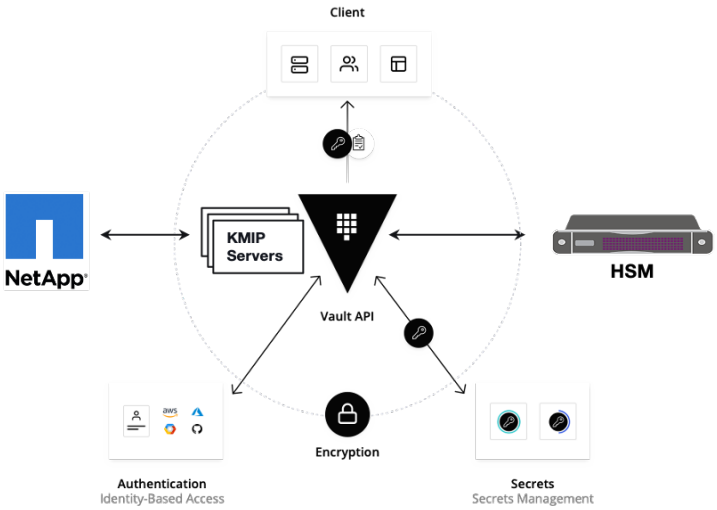
##Writing vault policy
```
vault policy write pki-policy -<<EOF
path "pki*" { capabilities = ["create", "read", "update", "delete", "list", "sudo"]}
EOF
```
##Write Auth role
```
vault write auth/approle/role/my-role secret_id_ttl=8760h token_num_uses=0 token_ttl=2160h token_max_ttl=8760h secret_id_num_uses=0 policies=pki-policy
```
##Note:-
##my-role - is the role name
##secret_id_ttl - (Optional) The number of seconds after which any SecretID expires
##token_num_uses - (Optional) The period, if any, in number of seconds to set on the token
##token_ttl - (Optional) The incremental lifetime for generated tokens in number of seconds. Its current value will be referenced at renewal time
##token_max_ttl - (Optional) The maximum lifetime for generated tokens in number of seconds. Its current value will be referenced at renewal time
##secret_id_num_uses - (Optional) The number of times any particular SecretID can be used to fetch a token from this AppRole, after which the SecretID will expire. ##A value of zero will allow unlimited uses.

##Read Auth role
##Here it will give you role id which you need to use in vault-approle-issuer.yml
```
vault read auth/approle/role/my-role/role-id
```
##Generate secret id
```
vault write -f auth/approle/role/my-role/secret-id
```
##By using above 2 command role id and secret id you need to pass in below command
```
vault write auth/approle/login role_id=<role-id> secret_id=<secret-id>
```
############################
##If the command successful then vault configuration and authentication via approle is completed
############################

##YAML files to be modified
##First execute below yaml file
```
kubectl apply -f cert-manager.yaml
```
##Need to replace with the latest secret id in base64 format by using below command
##Secret id already generate when we are executing vault command, need to use same secret id here
```
echo secret-id | base64
```
##The output of above command has to be replaced in the vault-apply-secret.yml file data.secretId
```
kubectl apply -f vault-apply-secret.yml
```
##No you will get one ip where your vault is running so that ip you can get by using below command
##Copy vault ip from below command
```
kubectl get svc
```
##Now vault ip and role id need to replace in vault-approle-issuer.yml file
##Role id already generated when we are executing vault commands
```
kubectl apply -f vault-approle-issuer.yml
```
##NOTE: spec.vault.server: IP here you need to change vault ip which you will get when u ren 'kubectl get svc'
##spec.vault.auth.roleId this is you need to replace and need to put latest role id which you get in 'vault read auth/approle/role/my-role/role-id'

##Then final we need to execute below yaml file
```
kubectl apply -f vault-cert-certificate.yml
```
##
Certificate generate process completed
##

##Now get ca certificate use below command
```
curl http://10.43.130.35:8200/v1/pki/ca/pem
```
##10.43.130.35 is your vault ip, need to replace with latest vault ip



Troubleshooting

N/A

Maintenance

Blueprint Package Maintenance

Software maintenance

N/A

Hardware maintenance

N/A

Blueprint Deployment Maintenance

N/A

Frequently Asked Questions

N/A

License

License information of EALTEdge Blueprint Components

OCD Host

CENTER Node

Center Node consists of 3 components . MECM , Appstore and Developer Portal.

Refer:

MECM Edge Gallery **http://docs.edgegallery.org/zh_CN/latest/Projects/MECM/MECM.html#**

S. No	Software	Type	Version	License	Remarks
1.	Docker	CRI	18.09	Apache 2.0 *license*	No code modifications done
2.	Kubernetes	Orchestration	v1.18.7	Apache 2.0 *license*	No code modifications done
3.	Edge Gallery	Opensource MEC Platform	1.1.1	Apache 2.0 *license*	No code modifications done

Edge Node

S. No	Software	Type	Version	License Information	Remarks
1.	Docker	CRI	18.09	Apache 2.0 *license*	No code modifications done
2.	K8s	Orchestration	1.18.7	Apache 2.0 *license*	No code modifications done
3.	Edge Gallery	Opensource MEC platform	1.1.1	Apache 2.0 *license*	Open Source MEC Platform

References

Definitions, acronyms and abbreviations

Abbreviations

- EALTEdge - Enterprise Application on Lightweight 5G Telco Edge (EALTEdge).
- MECM - Multi Access Edge Computing Manager.
- MEC - Multi Access Edge Computing.
- MEP - Multi Access Edge Platform.