

CloudSure OpenShift Test Environment

OpenShift 4.18.12 Bare Metal Installation (UPI Mode)

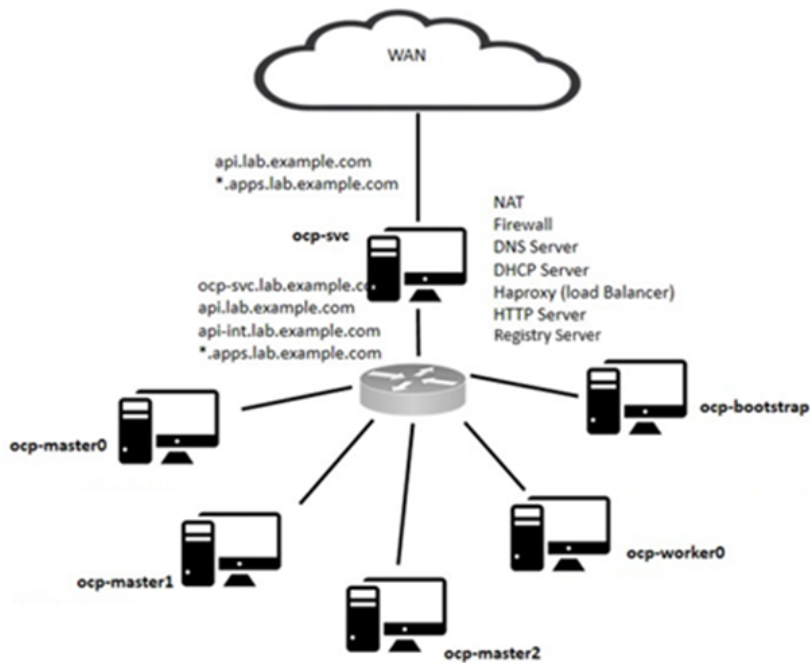
- [OpenShift 4.18.12 Bare Metal Installation \(UPI Mode\)](#)
 - [Implementation Details](#)
 - [High level Architecture diagram](#)
 - [Environment Setup](#)
 - [Network Diagram](#)
 - [Cable Mapping](#)
 - [Network Information](#)
 - [Network Services](#)
 - [Internet Access](#)
 - [Storage Information](#)
 - [Certificates](#)
 - [Red Hat OpenShift Container Platform 4 - Logical HA Architecture](#)
 - [Bare Metal Infrastructure Specification](#)
 - [Bastion Node Configuration and Technical Implementation](#)

Overview

This guide provides a step-by-step process for installing OpenShift Container Platform (OCP) version **4.18.12** on **bare metal servers** using the **User Provisioned Infrastructure (UPI)** method. The deployment uses **RHEL 9** for the bastion node and **RHCOS 4.18.1** for control and compute nodes.

The process includes:

- Setting up core infrastructure services (DHCP, TFTP, HTTP, Load Balancer)
- Mirroring the OpenShift registry to a local Quay instance
- PXE booting RHCOS on the nodes
- Running the installer and approving node CSRs



Implementation Details

Deployed Architecture

Architecture and design for Spirent is covered in the design document (LLD) and should be referenced before proceeding further. Below diagram has been picked from the same.

High level Architecture diagram

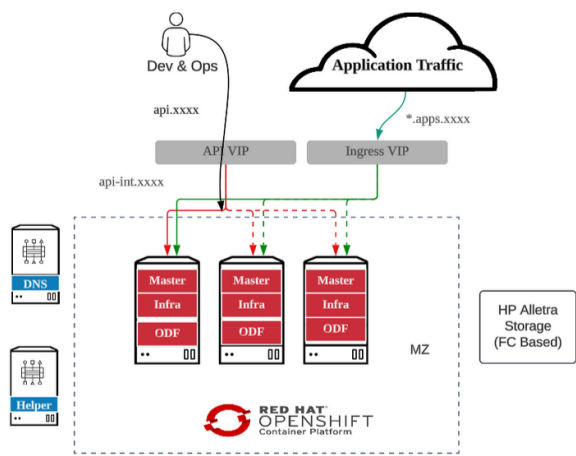
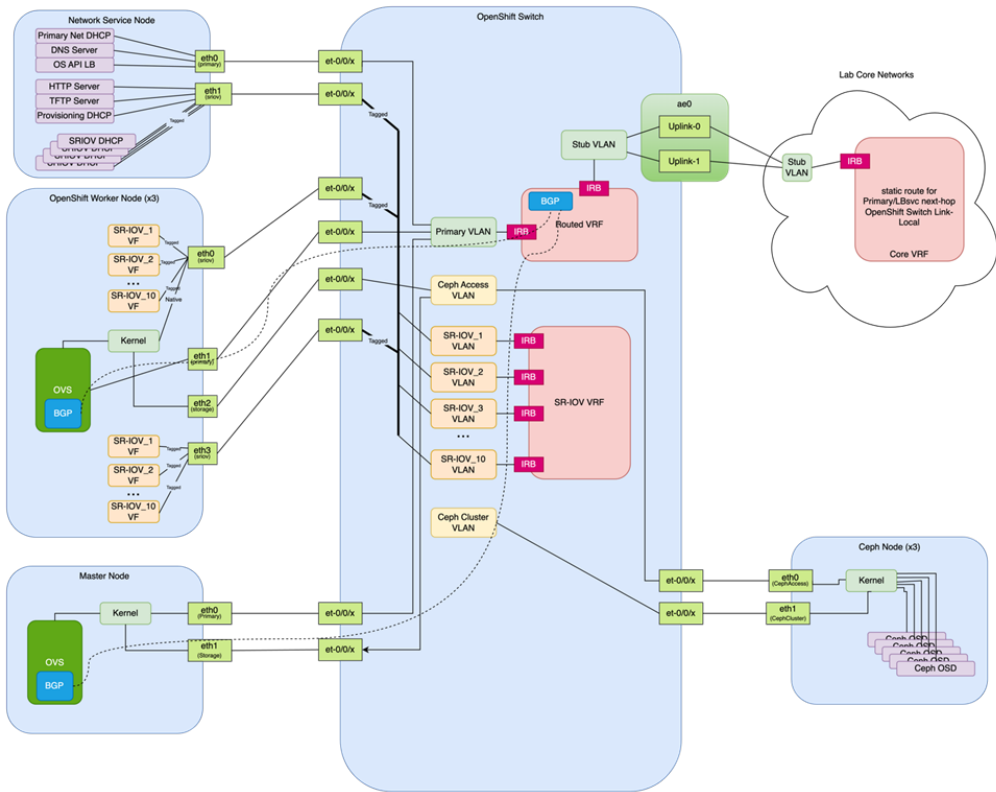


Figure 1. NonProd OCP Deployment Architecture (DEV)

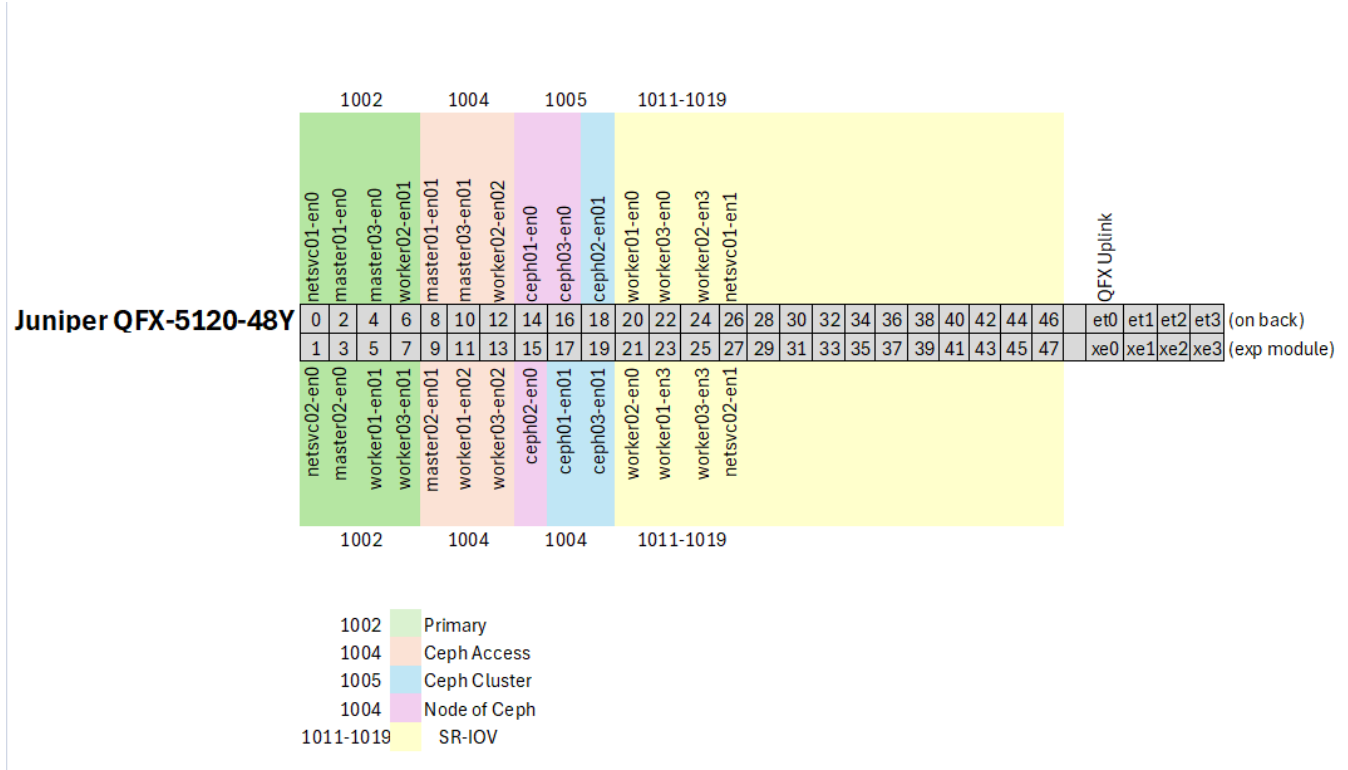
Environment Setup

Steps to prepare or create the environment for the proposed architecture

Network Diagram



Cable Mapping



Network Information

Table 1. Network Data

Name	IP Address Pool	Comments
Cluster Network	172.16.0.0/16	Non Routable
Service Network	172.17.0.0/16	Non Routable
Host Network	10.224.225.0/24	Routable

Network Services

Table 2. Network Service Data

Services	Host	Comments
DNS Server	provided by spirent	Nameserver IP for OCP nodes.
DHCP Server	N/A	Static IPs will be used for OCP nodes

Load Balancer Config Details

Table 3. Load Balancer Data

VIP	URL	Port	Type
10.224.226.0/24	api.ocp01.calenglab.spirentcom.com	6443,22623	Passtthrough (layer 4 routing)
10.224.226.0/24	api-int.ocp01.calenglab.spirentcom.com	6443,22623	Passtthrough (layer 4 routing)
10.224.226.0/24	*.apps.ocp01.calenglab.spirentcom.com	80,443	Passtthrough (layer 4 routing)

Internet Access

The RHOCP-4.18.12 is a disconnected mode implementation where internet access is provided on the Bastion node using an Internet to download mirror images and required packages.

Node Information

Table 4. Nodes Data

Server FQDN(e.g)	IP	Role	Subs Used	OS
master01.ocp01.calenglab.spirentcom.com	10.224.225.0/24	controlplane,master,worker	N/A	RHCOS
master02.ocp01.calenglab.spirentcom.com	10.224.225.0/24	controlplane,master,worker	N/A	RHCOS
master03.ocp01.calenglab.spirentcom.com	10.224.225.0/24	controlplane,master,worker	N/A	RHCOS
worker01.ocp01.calenglab.spirentcom.com	10.224.225.0/24	worker	N/A	RHCOS
worker02.ocp01.calenglab.spirentcom.com	10.224.225.0/24	worker	N/A	RHCOS
worker03.ocp01.calenglab.spirentcom.com	10.224.225.0/24	worker	N/A	RHCOS

Storage Information

Table 5. Storage Data

Application	Storage Type	CSI Driver	Mount Path	Size
Registry	File	RHOCS ODF	/registry	200Gi
Monitoring	Block	RHOCS ODF	prometheus	1000Gi
Monitoring	Block	RHOCS ODF	user-prometheus-0	300Gi
Alert-Manager	Block	RHOCS ODF	/alertmanager	10Gi
Application	Block	RHOCS ODF	N/A	1000Gi

Certificates

Spirent at source has planned to use self signed certificates by their internal CA forWild Card (*.apps) Domain Ingress Controller.

Red Hat OpenShift Container Platform 4 - Logical HA Architecture

All OpenShift environments for on prem environments will utilize hardware to achieve some level of redundancy. Each master and infrastructure component (EFK, metrics, router, and registry) should reside on different physical hardware. The image below illustrates a simple cluster example.

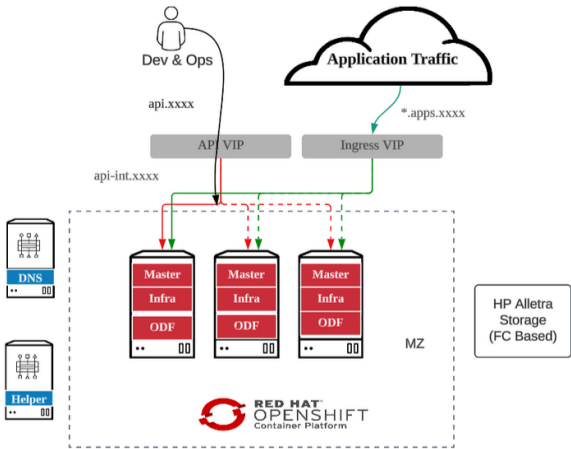


Figure 2. Cluster Diagram

Bare Metal Infrastructure Specification

Machine	OS	CPU	RAM (GB)	Storage (GB)
Bastion Node	RHEL 9	4	32	200+
Bootstrap Node	rhcos-4.18.1-x86_64-live.x86_64.iso	4	10	100
Master-1 Node	rhcos-4.18.1-x86_64-live.x86_64.iso	4	32	200+
Master-2 Node	rhcos-4.18.1-x86_64-live.x86_64.iso	4	32	200+
Master-3 Node	rhcos-4.18.1-x86_64-live.x86_64.iso	4	32	200+
Worker-1 Node	rhcos-4.18.1-x86_64-live.x86_64.iso	16	256	200+
Worker-2 Node	rhcos-4.18.1-x86_64-live.x86_64.iso	16	256	200+
Worker-3 Node	rhcos-4.18.1-x86_64-live.x86_64.iso	16	256	200+

3. Required Downloads

A. OpenShift CLI and Installer

- openshift-client-linux-4.18.12.tar.gz
- openshift-install-linux-4.18.12.tar.gz

B. Registry & Mirror Tools

- mirror-registry.tar.gz
- oc-mirror.tar.gz
- opm-linux-4.18.12.tar.gz

C. System Tools

- butane-amd64

D. OS ISO

- rhcos-4.18.1-x86_64-live.x86_64.iso
- Download all from:
<https://mirror.openshift.com/pub/openshift-v4/>

Bastion Node Configuration and Technical Implementation

Check Bastion Node for all the pre-Installation requirements

Operating System Details

```
cat /etc/redhat-release
```

Block Device (Hard Disk) Details

```
df -h
```

Checking hostname.

```
hostname
```

resolve nameserver

```
cat /etc/resolv.conf
```

Route and Default Gateway Details

```
ip r
```

Checking IP address

```
ip a
```

Enabling Yum Repositories

```
yum repolist
```

Checking ocp binary version

```
oc version
```

Checking openshift-install binary version

```
openshift-install version
```

Checking DNS records

```
for a in 10.50.164.{11..22}; do dig -x $a +short ; done

for a in master{01..03}.ocp01.calenglab.spirentcom.com.in worker{01..04}.ocp01.calenglab.spirentcom.com; do dig $a
```

A) DHCP Server Setup

```
yum install dhcp-server -y

vim /etc/dhcp/dhcpd.conf

echo 'DHCPDARGS="ens224"' >> /etc/sysconfig/dhcpd

systemctl start dhcpd && systemctl enable dhcpd
```

B) Haproxy Server Setup

```
yum install haproxy* -y
```

```
vim /etc/haproxy/haproxy.cf

global
    log          127.0.0.1 local2

    pidfile      /var/run/haproxy.pid

    maxconn      4000

    daemon

defaults
    mode          http

    log           global
```

```
option                        dontlognull

option http-server-close

option                        redispatch

retries                       3

timeout http-request         10s

timeout queue                1m

timeout connect              10s

timeout client               1m

timeout server               1m

timeout http-keep-alive 10s

timeout check                10s

maxconn                      3000

frontend stats

    bind *:1936

    mode                http

    log                 global

    maxconn 10

    stats enable

    stats hide-version

    stats refresh 30s

    stats show-node

    stats show-desc Stats for ocp4 cluster

    stats auth admin:ocp4

    stats uri /stats

listen api-server-6443

    bind *:6443

    mode tcp

    server bootstrap bootstrap.ocp01.calenglab.spirentcom.com:6443 check inter 1s backup

    server master1 master1.ocp01.calenglab.spirentcom.com:6443 check inter 1s

    server master2 master2.ocp01.calenglab.spirentcom.com:6443 check inter 1s

    server master3 master3.ocp01.calenglab.spirentcom.com:6443 check inter 1s

listen machine-config-server-22623

    bind *:22623

    mode tcp
```

```
server bootstrap bootstrap.ocp01.calenglab.spirentcom.com:22623 check inter 1s backup

server master1 master1.ocp01.calenglab.spirentcom.com:22623 check inter 1s

server master2 master2.ocp01.calenglab.spirentcom.com:22623 check inter 1s

server master3 master3.ocp01.calenglab.spirentcom.com:22623 check inter 1s


listen ingress-router-443

    bind *:443

    mode tcp

    balance source

    server worker1 master1.ocp01.calenglab.spirentcom.com:443 check inter 1s

    server worker2 master2.ocp01.calenglab.spirentcom.com:443 check inter 1s

    server worker3 master3.ocp01.calenglab.spirentcom.com:443 check inter 1s


listen ingress-router-80

    bind *:80

    mode tcp

    balance source

    server worker1 master1.ocp01.calenglab.spirentcom.com:80 check inter 1s

    server worker2 master2.ocp01.calenglab.spirentcom.com:80 check inter 1s

    server worker3 master3.ocp01.calenglab.spirentcom.com:80 check inter 1s
```

```
systemctl start haproxy

systemctl enable haproxy

systemctl status haproxy

setsebool -P haproxy_connect_any 1

setenforce 0

systemctl restart haproxy
```

C) Apache Web Server Setup

Install apache web server for bootable media url.

- Installing and Configuring httpd packages.

```
yum install httpd -y
```



```
sed -i 's/Listen 80/Listen 0.0.0.0:8080/' /etc/httpd/conf/httpd.conf

firewall-cmd --add-port=8080/tcp --zone=internal --permanent

firewall-cmd --reload

systemctl enable httpd

systemctl start httpd
```

D) Quay Mirror Registry

For installing Quay:-

```
tar xf mirror-registry.tar.gz -C /usr/bin/

tar xf oc-mirror.tar.gz -C /usr/bin/

tar xf openshift-client-linux-4.18.12.tar.gz -C /usr/bin/

tar xf opm-linux-4.18.12.tar.gz -C /usr/bin/

cp mirror-registry.tar.gz /ocpreistry

cd /ocpreistry

tar xf mirror-registry.tar.gz

./mirror-registry install --quayHostname registry.ocp4.siprent.com --initUser openshift --initPassword redhat123

systemctl disable --now firewalld

podman image ls

podman ps

podman login -u openshift -p redhat123 https:// registry.ocp4.lab.siprent.com:8443
```

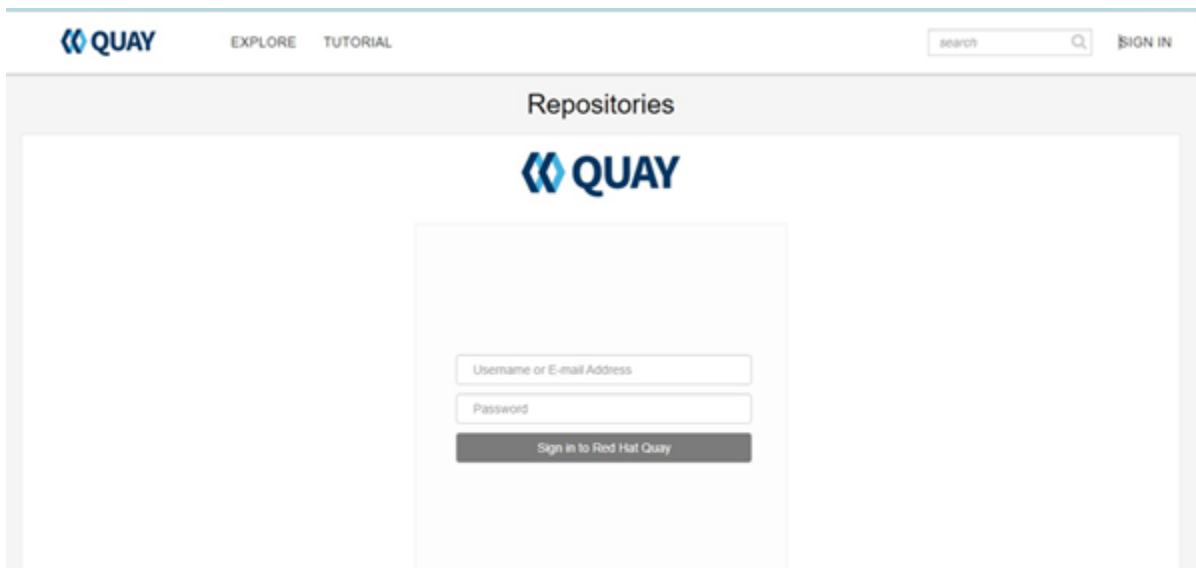
check URL <https://registry.ocp01.calenglab.siprentcom.com:8443> on browser end.

(If got any certificate error, then follow below steps)

```
cp /ocpreistry/quay-rootCA/rootCA.pem /etc/pki/ca-trust/source/anchors/

update-ca-trust

podman login --authfile quay-secret.json -u openshift -p redhat123 https://registry.ocp01.calenglab.siprentcom.com:8443
```



To setup for adding OCP Base to Register end:-

Add below env. Into bashrc

```
vi .bashrc

export OCP_RELEASE=4.18.12

export LOCAL_REGISTRY=registry.ocp01.calenglab.spirentcom.com:8443

export LOCAL_REPOSITORY=ocp4/openshift4

export PRODUCT_REPO='openshift-release-dev'

export RELEASE_NAME="ocp-release"

export ARCHITECTURE=x86_64

export REMOVABLE_MEDIA_PATH=/openshift/ocp-base-images

export REG_CREDS=/root/quay-secret.json

export GODEBUG=x509ignoreCN=0

source .bashrc
```

Use this command when you have OCP-Base image on local end then push it to registry end.

```
oc image mirror -a ${LOCAL_SECRET_JSON} -from-dir=${REMOVABLE_MEDIA_PATH}/mirror file://openshift
/release:${OCP_RELEASE}* ${LOCAL_REGISTRY}/${LOCAL_REPOSITORY}
```

E) TFTP Installation Setup

- Install TFTP server

```
dnf install tftp-server
```

- Create pxelinux directory as below

```
mkdir /var/lib/tftpboot/pxelinux
```

- Install Kernel, rootfs, initramfs images choose x86 version in this path /var/lib/tftpboot/pxelinux using wget utility
- Using below command to get image links

```
openshift-install coreos print-stream-json | grep -Eo "https.*(kernel-|initramfs.|rootfs.)\w+(\.img)?"  
  
wget https://rhcos.mirror.openshift.com/art/storage/prod/streams/4.13-9.2/builds/413.92.202305021736-0/x86_64/rhcos-413.92.202305021736-0-live-kernel-x86_64
```

- Create a prelinux.cfg dir to keep images and create a default file and copy contents as per below file and edit img details and mention HTTP server ip

```
mkdir -p /var/lib/tftpboot/pxelinux/pxelinux.cfg  
  
touch default(file creation)
```

- Copy Kernel, rootfs, initramfs images to /var/www/html/rhocp413 from #/var/lib/tftpboot/pxelinux

```
cp rhcos-413.92.202305021736-0-live-initramfs.x86_64.img rhcos-413.92.202305021736-0-live-kernel-x86_64 rhcos-413.92.202305021736-0-live-rootfs.x86_64.img /var/www/html/rhocp/
```

- Create a file in /var/lib/tftpboot/pxelinux as boot.msg and copy & paste contents as below file.

```
touch boot.msg
```

- Get the below drivers (initrd.img, ldlinux.c32, pxelinux.0, vmlinuz) with the following steps.

- Mount the rhel os image in any directory (to get the initrd.img, ldlinux.c32, vmlinuz)

```
mkdir mounting
```

- Place the rhel os image in that mounting directory (in the picture I've used rhel 8.4 to get that drivers)
- Mount the image in that directory

```
mount -o loop /root/mounting/rhel-8.4-x86_64-dvd.iso /root/mounting/
```

- After mounting, this is how your directory will look like
- Go to isolinux directory, you will get the three drivers except pxelinux.0
- Copy and paste the drivers (mentioned in the above image) in this /var/lib/tftpboot/pxelinux path
- After copied the images unmount the disk

```
umount /root/mounting
```

- To get the pxelinux.0 driver, install syslinux package

```
yum install syslinux
```

- Go to /usr/share/syslinux (copy the pxelinux.0 driver) and paste it in this /var/lib/tftpboot/pxelinux path
- Change permissions to files in this /var/lib/tftpboot/pxelinux path using below cmd

```
chown nobody:nobody *
```

- Start, enable and check status of TFTP service

```
systemctl start tftp.service  
systemctl enable tftp.service  
systemctl status tftp.service
```

5. OCP 4.18.12 Installation

A. Install Config Preparation

```
tar -xvf openshift-install-linux-4.18.12.tar.gz

cp openshift-install /usr/bin

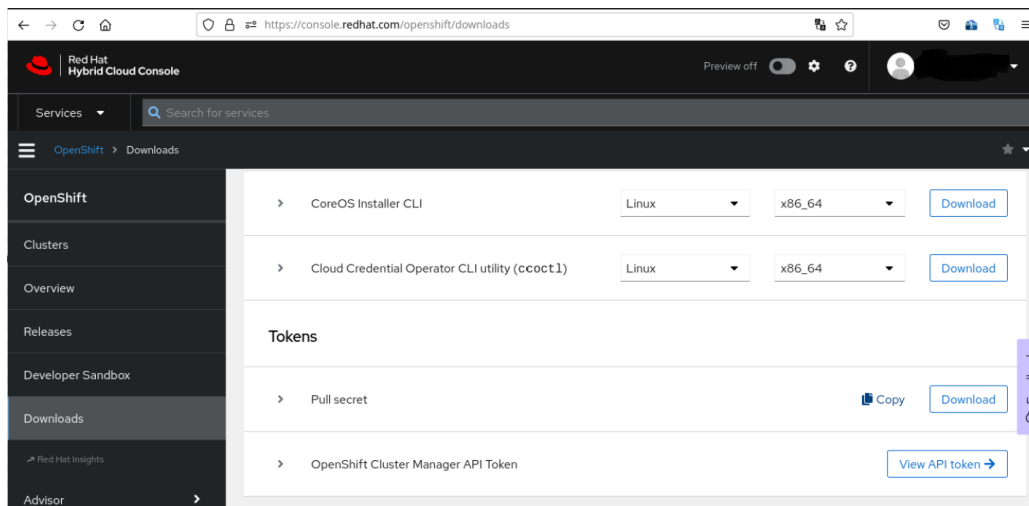
ssh-keygen -t rsa -b 4096 -N ''

cat .ssh/id_rsa.pub
```

Installing a OpenShift Cluster in a Disconnected Network on Baremetal Machines

Gathering pull secret file.

Login to RedHat Hybrid Cloud Console. <https://cloud.redhat.com/openshift/downloads>



Creating Install config yaml

- Create install-config.yaml file for bare metal.

```
vim install-config.yaml
```

```
apiVersion: v1

baseDomain: spirent.com

compute:
- hyperthreading: Enabled
  name: worker
  replicas: 0

controlPlane:
  hyperthreading: Enabled
  name: master
  replicas: 3

metadata:
  name: lab

networking:
  clusterNetwork:
  - cidr: 10.46.0.0/16
    hostPrefix: 23
  networkType: OpenShiftSDN
  serviceNetwork:
  - 10.47.0.0/16

platform:
  none: {}

fips: false

pullSecret: ''

sshKey: ""

additionalTrustBundle: |
  -----BEGIN CERTIFICATE-----

  -----END CERTIFICATE-----

imageContentSources:
- mirrors:
  - registry.ocp01.calenglab.spirentcom.com:8443/ocp4/openshift4
    source: quay.io/openshift-release-dev/ocp-release
- mirrors:
  - registry.ocp01.calenglab.spirentcom.com:8443/ocp4/openshift4
    source: quay.io/openshift-release-dev/ocp-v4.0-art-dev
```

Note:-

In the above 'install-config.yaml', don't forget to change the following details:

- pullSecret : Get it from cat quay-secret.json
- sshKey : Get it from cat /.ssh/id_rsa.pub
- additionalTrustBundle : cat /ocpregistry/quay-rootCA/rootCA.pem

B. Creating Manifests and Ignition Files

Creating nonprod-ocp base directory where included install-config and add these ignitions to httpd server path end for browsing.

```
mkdir ocp01

cp install-config.yaml ocp01/

openshift-install create manifests --dir=ocp01

openshift-install create ignition-configs --dir=nonprod-ocp

cd ocp01/

cp -rf * /var/www/html/ocp01/

chown -R apache: /var/www/html/ocp01/

chmod -R 755 /var/www/ocp01/

restorecon -RFv /var/www/html/ocp01/

curl localhost:8080/ocp01/
```

after installation complete by iPXE boot mode,

then goto your bastion machine, use these below steps on bootstrap,

C. Monitoring Bootstrap

Waiting bootkube complete and Waiting bootstrap completion.

```
ssh core@bootstrap

journalctl

~/openshift-install --dir ~/ocp01 wait-for bootstrap-complete --log-level=debug
```

For checking node/cluster status and approving pending certificates for worker node

D. Node Certificate Approval

Export Kubeconfig file and Getting Cluster node status.

```

export KUBECONFIG=~/.odf/auth/kubeconfig

oc get nodes

oc get co

oc get csr

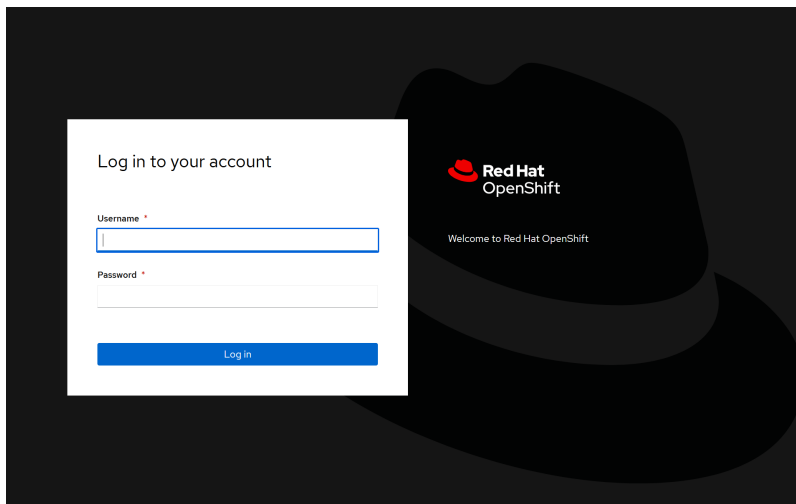
for i in `oc get csr --no-headers | grep -i pending | awk '{ print $1 }'`; do oc adm certificate approve $i; done

for i in `oc get csr --no-headers | grep -i serving | awk '{ print $1 }'`; do oc adm certificate approve $i; done

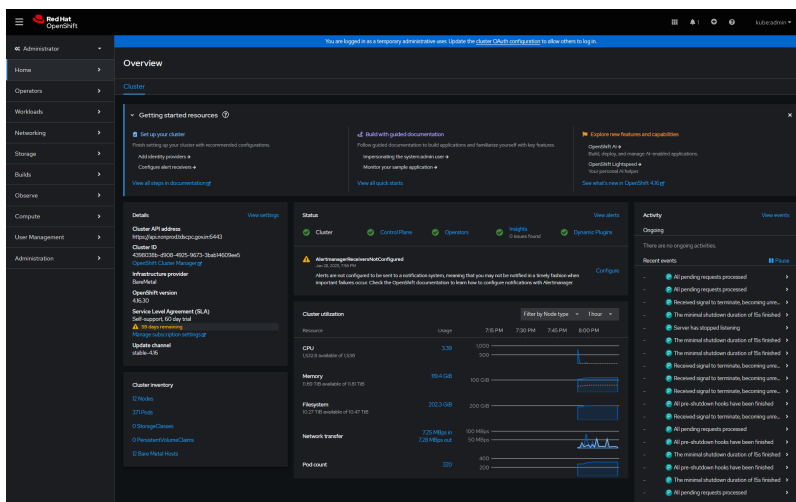
oc get clusterversion

```

OpenShift Login Console



OpenShift Dashboard



6. Operator Catalog Mirroring (Optional)

List all available Operator in a catalog

```
./bin/oc-mirror list operators --catalog=registry.redhat.io/redhat/redhat-operator-index:v4.18
```


Create one yaml with name isc.yaml

```
vi isc.yaml
```

```
kind: ImageSetConfiguration
apiVersion: mirror.openshift.io/v2alpha1
mirror:
  platform:
    channels:
      - name: stable-4.18
        minVersion: '4.18.12'
        maxVersion: '4.18.12'
        shortestPath: true
        type: ocp
  operators:
    - catalog: registry.redhat.io/redhat/redhat-operator-index:v4.18
      packages:
        - name: lvms-operator
          channels:
            - name: stable-4.18
        - name: local-storage-operator
          channels:
            - name: stable
        - name: loki-operator
          channels:
            - name: stable-6.2
        - name: cluster-logging
          channels:
            - name: stable-6.2
        - name: elasticsearch-operator
          channels:
            - name: stable-5.8
        - name: kubevirt-hyperconverged
          channels:
            - name: stable
```

```
- name: kubernetes-nmstate-operator

  channels:

    - name: stable

- name: mtv-operator

  channels:

    - name: release-v2.8

- name: metallb-operator

  channels:

    - name: stable
```

Mirror to Disk

```
oc-mirror -c ./isc.yaml file:///root/quay-ops/oc-mirror/mirror1 --v2
```

Disk to Mirror

```
oc-mirror -c ./isc.yaml --from file:///root/quay-ops/oc-mirror/mirror1 docker://kvmhost-raven.blackbird.com:8443 --v2
```