

Openshift Container Platform

Detail Installation Document (DID)

Preparado para: Claro

INDICE

[INDICE](#)

[INTRODUCCIÓN](#)

[OBJETIVO DEL DOCUMENTO](#)

[AUDIENCIA](#)

[ARQUITECTURA](#)

[Diagrama de la solución](#)

[Componentes de la solución](#)

[Openshift Clusters](#)

[Detalle de hardware](#)

[Listado de Servidores](#)

[Sistema Operativo](#)

[MASTER - Configuración general](#)

[Información general](#)

[Particionado de disco SO](#)

[Particionado de disco Datos](#)

[Configuración LVM](#)

[NODO - Configuración general](#)

[Información general](#)

[Particionado de disco SO](#)

[Particionado de disco Datos](#)

[Configuración LVM](#)

[Bastión - Configuración general](#)

[Información general](#)

[Particionado de disco SO y configuración LVM](#)

[Storage Persistente](#)

[Certificados SSL](#)

[Autenticación de usuarios](#)

[DNS y Balanceo de carga](#)

[INSTALACIÓN](#)

[Plan de Acción \(POA\)](#)

[Preparación de los servidores](#)

[Suscripciones y repositorios](#)

[Repositorios](#)

[Acceso a los servidores](#)

[Instalación de paquetes RPM](#)

[Docker Storage](#)

[Openshift Deploy](#)

[Armado de Inventory File](#)

[Instalación de Openshift](#)

[Tareas post-instalación](#)

[Tareas post-cluster-deploy](#)

[Privilegios administración del cluster](#)

[Integración con Cloudforms](#)

[Configurar Capacity & Utilization](#)

[Habilitar Smartstate Analysis](#)

[Alta del Container Provider](#)

[Openshift Summary](#)

[Logcollector y Backup](#)

[ANEXO A - ANSIBLE FILES](#)

[CONTROL DEL DOCUMENTO](#)

[Contribuidores](#)

[Revisiones](#)

CONFIDENTIALITY, COPYRIGHT AND DISCLAIMER

This is a Customer-facing document between Red Hat, Inc. and CLARO (“Client”).

Copyright © 2018 Red Hat, Inc. All Rights Reserved. No part of the work covered by the copyright herein may be reproduced or used in any form or by any means – graphic, electronic, or mechanical, including photocopying, recording, taping, or information storage and retrieval systems – without permission in writing from Red Hat except as is required to share this information as provided with the aforementioned confidential parties.

This document is not a quote and does not include any binding commitments by Red Hat.

INTRODUCCIÓN

OBJETIVO DEL DOCUMENTO

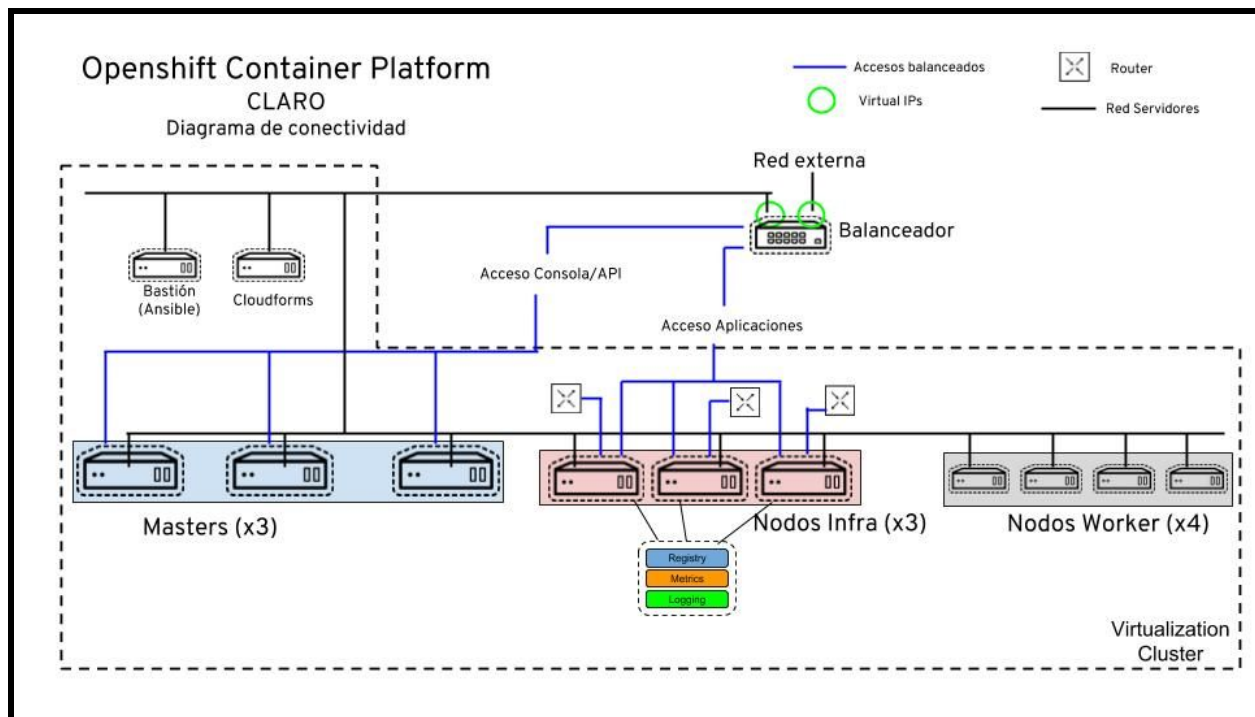
El presente documento tiene como objetivo proporcionar una vista de estado final de la implementación de la solución de Red Hat OpenShift Container Platform (RH OCP) y Red Hat Cloudforms (RH CFME), componentes de la infraestructura Cloud de Red Hat para el proyecto de CLARO.

AUDIENCIA

El presente documento está dirigido a los gerente de proyecto y staff técnico del cliente responsable de la planificación y preparación de los componentes necesarios de la infraestructura Red Hat Openshift Container Platform.

ARQUITECTURA

Diagrama de la solución



Componentes de la solución

La solución está compuesta de los siguientes servidores

Openshift Clusters

Cantidad de clusters: 2

Ambientes: Producción y noProducción

Cada cluster está compuesto por:

- **Tres (3) Masters:** componente que provee una API, orquestación de servicios, mantenimiento de estados y administración de Servicios y Pods.
- **Siete (7) Nodos:** destinados a instanciar los containers de infraestructura (Registry, Router, Metrics, Logging) y de Aplicaciones. Tres nodos serán asignados como infraestructura y cuatro se asignan para instanciar Aplicaciones.

Además se utilizarán estos servidores adicionales:

- **Un (1) Bastión:** componente destinado a realizar la instalación de la plataforma utilizando Ansible. Cumplirá también el rol de repositorio de RPMs temporal para utilizar al momento de la instalación.
- **Un (1) Cloudforms:** cumple la función de administración y reporte de los clusters Openshift

Nota:

Todos estos servidores serán máquinas virtuales VMware, disponibilizadas por el Cliente según lineamientos de Redhat.

Detalle de hardware

Detalle de los recursos de hardware virtual asignado a los servidores

Masters

| | |
|-----------------|---|
| CPU | 4 vCPU |
| MEM | 16 GB |
| Discos Internos | 1x 80GB (SO) 1x 100GB (docker) |
| Red | 3x vNIC (Red Servicio, Management y Backup) |

Nodos

| | |
|-----------------|--|
| CPU | 16 vCPU |
| MEM | 64 GB |
| Discos Internos | 1x 80GB (SO) 1x 100GB (docker) 1x 300GB (logging)* |
| Red | 3x vNIC (Red Servicio, Management y Backup) |

* Solamente los Nodos infra tendrán un disco adicional de 300GB

Bastión

| | |
|-----------------|---|
| CPU | 2 vCPU |
| MEM | 8 GB |
| Discos Internos | 1x 80GB (SO) 1x 200GB (Repositorio RPMs) |
| Red | 3x vNIC (Red Servicio, Management y Backup) |

Cloudforms

| | |
|-----------------|---|
| CPU | 4 vCPU |
| MEM | 16 GB |
| Discos Internos | 1x 44GB (SO) 1x 100GB (Database) |
| Red | 3x vNIC (Red Servicio, Management y Backup) |

NOTA

Cloudforms es un Appliance Virtual y se genera a través de una imagen OVA, tanto la Máquina Virtual como la instalación del Sistema Operativo y el Cloudforms propiamente dicho.

Listado de Servidores

| Ambiente | Nombre | Dominio | IP Red Servicio | IP Red Management | IP Red Backup |
|----------|------------------|------------|-----------------|-------------------|---------------|
| PROD | osep01-master-01 | .claro.amx | 10.92.84.80 | 10.111.34.215 | 10.111.129.60 |
| | osep01-master-02 | .claro.amx | 10.92.84.81 | 10.111.34.216 | 10.111.129.61 |
| | osep01-master-03 | .claro.amx | 10.92.84.82 | 10.111.34.217 | 10.111.129.62 |
| | osep01-infra-01 | .claro.amx | 10.92.84.83 | 10.111.34.218 | 10.111.129.63 |
| | osep01-infra-02 | .claro.amx | 10.92.84.84 | 10.111.34.219 | 10.111.129.64 |
| | osep01-infra-03 | .claro.amx | 10.92.84.85 | 10.111.34.220 | 10.111.129.65 |
| | osep01-worker-01 | .claro.amx | 10.92.84.86 | 10.111.34.221 | 10.111.129.66 |
| | osep01-worker-02 | .claro.amx | 10.92.84.87 | 10.111.34.222 | 10.111.129.67 |
| | osep01-worker-03 | .claro.amx | 10.92.84.88 | 10.111.34.223 | 10.111.129.68 |
| | osep01-worker-04 | .claro.amx | 10.92.84.89 | 10.111.34.224 | 10.111.129.69 |
| noPROD | osen01-master-01 | .claro.amx | 10.92.84.90 | 10.111.34.225 | 10.111.129.70 |
| | osen01-master-02 | .claro.amx | 10.92.84.91 | 10.111.34.226 | 10.111.129.71 |
| | osen01-master-03 | .claro.amx | 10.92.84.92 | 10.111.34.227 | 10.111.129.72 |
| | osen01-infra-01 | .claro.amx | 10.92.84.93 | 10.111.34.228 | 10.111.129.73 |
| | osen01-infra-02 | .claro.amx | 10.92.84.94 | 10.111.34.229 | 10.111.129.74 |
| | osen01-infra-03 | .claro.amx | 10.92.84.95 | 10.111.34.230 | 10.111.129.75 |
| | osen01-worker-01 | .claro.amx | 10.92.84.96 | 10.111.34.231 | 10.111.129.76 |
| | osen01-worker-02 | .claro.amx | 10.92.84.97 | 10.111.34.232 | 10.111.129.77 |
| | osen01-worker-03 | .claro.amx | 10.92.84.98 | 10.111.34.233 | 10.111.129.78 |
| | osen01-worker-04 | .claro.amx | 10.92.84.99 | 10.111.34.234 | 10.111.129.79 |
| ambos | cfme01 | .claro.amx | 10.92.84.78 | 10.111.34.235 | 10.111.129.80 |
| ambos | ose01-bastion | .claro.amx | 10.92.84.79 | 10.111.34.214 | 10.111.129.59 |

Listado de Virtual IPs utilizadas para balancear el acceso a los Masters y Nodos Infra

| Nombre | Dominio | IP Red Servicio |
|-------------------|-----------|-----------------|
| osep01-api | claro.amx | 10.92.55.191 |
| osep01-api-int | claro.amx | 10.92.55.192 |
| *.osep01-apps | claro.amx | 10.92.55.189 |
| *.osep01-apps-ssl | claro.amx | 10.92.55.190 |
| osen01-api | claro.amx | 10.105.218.69 |
| osen01-api-int | claro.amx | 10.105.218.70 |
| *.osen01-apps | claro.amx | 10.105.218.67 |
| *.osen01-apps-ssl | claro.amx | 10.105.218.68 |

Configuración general de red

| Parámetro | Valor | Notas |
|-------------------|--|---|
| Default Gateway | 10.92.84.1 | Corresponde al gateway de la Red de Servicio |
| DNS Servers | 10.92.55.39 10.92.48.108 | |
| NTP Servers | ntpdserv-a.claro.amx ntpdserv-b.claro.amx | |
| Domain | claro.amx | Dominio interno utilizado para los servidores |
| Apps Subdomain | *.osep01-apps.claro.amx *.osen01-apps.claro.amx *.osep01-apps-ssl.claro.amx *.osen01-apps-ssl.claro.amx | Es el subdominio por defecto donde se exponen las Apps desde Openshift Los que contienen '-ssl' se utilizaron para los servicios propios de la plataforma |
| Acceso a Internet | El acceso a internet será ruteado a través del Default Gateway y estará habilitado sólo para la etapa de implementación. | Se debe habilitar el acceso a los siguientes sitios: <ul style="list-style-type: none"> • *.redhat.com • *.akamaiedge.net • *.docker.com • *.github.com • *.maven.org • *.apache.org • *.npmjs.com • *.openshift.io • *.openshift.org • *.docker.io • *.docker.org • *.rubygems.org • *.cpan.org • *.githubusercontent.com • *.githubapp.com • *.getcomposer.org • *.github.io • *.cloudfront.net |

Detalle de Redes

| Nombre | Subnet | Gateway | Vlan ID | Descripción |
|---------------------|----------------------------------|-------------|---------|---|
| Servicio | 10.92.84.0/24 | 10.98.84.1 | 37 | Red para los servidores Openshift PROD Será utilizada como Default Route para acceder a los servicios externos, como DNS, NTP, LDAP, Bases de Datos y demás. Sobre esta interfaz se configura el Switch Virtual que controla la SDN (openvswitch) |
| Management | 10.111.34.0/24 | 10.111.34.1 | 96 | Red de Management |
| Backup | 10.111.129.0/22 | N/A | 54 | Red de Backup |
| Portal/Servicio | 10.92.240.0/21 10.92.248.0/21 | N/A | N/A | SDN network para recursos Service, balanceo interno de los containers |
| Cluster/Pods PROD | 10.128.0.0/20 | N/A | N/A | SDN network para los containers PROD |
| Cluster/Pods noPROD | 10.129.0.0/20 | N/A | N/A | SDN network para los containers noPROD |

Sistema Operativo

Lineamientos generales para la configuración del Sistema Operativo

MASTER - Configuración general

A continuación se describe la configuración general de las máquinas que actuarán como Masters.

Información general

| | |
|-------------------|-------------------------------------|
| Root Password | root00 |
| Sistema Operativo | Red Hat Enterprise Linux 7.5 x86_64 |
| Firewall | Enabled |
| SELinux | Enforcing |
| Lang | en_US.UTF-8 |
| Keyboard | US |
| Timezone | America/Argentina/Buenos Aires |
| Packages | Base |

Particionado de disco SO

| Partición | Tamaño | Mount | FS | Descripción |
|-----------|---------|------------|-----|-------------|
| 1 | 1024 MB | /boot | XFS | Boot FS |
| 2 | [Resto] | [LVM vg00] | - | LVM |

Particionado de disco Datos

| Partición | Tamaño | Mount | FS | Descripción |
|-----------|--------|--------------------|----|-------------|
| 1 | [Todo] | [LVM docker-vg] | - | LVM |

Configuración LVM

| VG | LV | Size | Mount | FS | Descripción |
|-----------|-------------|--------|------------|--------|-------------|
| vg00 | root | 4GB | / | XFS | Root FS |
| | var | 45GB | /var | XFS | Var FS |
| | home | 2GB | /home | XFS | |
| | tmp | 2GB | /tmp | XFS | |
| | usr | 7GB | /usr | XFS | |
| | opt | 5GB | /opt | XFS | |
| | openv | 5GB | /usr/openv | XFS | |
| | swap | 8GB | swap | [SWAP] | Swap |
| docker-vg | docker-pool | [todo] | N/A | - | Docker |

NOTA

Tanto el VG como el LV de **docker** será creado por el script `docker-storage-setup` mencionado en las próximas secciones.

NODO - Configuración general

A continuación se describe la configuración general de las máquinas que actuarán como Nodo.

Información general

| | |
|-------------------|-------------------------------------|
| Root Password | root00 |
| Sistema Operativo | Red Hat Enterprise Linux 7.5 x86_64 |
| Firewall | Enabled |
| SELinux | Enforcing |
| Lang | en_US.UTF-8 |
| Keyboard | US |
| Timezone | America/Argentina/Buenos Aires |
| Packages | Base |

Particionado de disco SO

| Partición | Tamaño | Mount | FS | Descripción |
|-----------|---------|------------|-----|-------------|
| 1 | 1024 MB | /boot | XFS | Boot FS |
| 2 | [Resto] | [LVM vg00] | - | LVM |

Particionado de disco Datos

| Partición | Tamaño | Mount | FS | Descripción |
|-----------|--------|--------------------|----|-------------|
| 1 | [Todo] | [LVM docker-vg] | - | LVM |

Configuración LVM

| VG | LV | Size | Mount | FS | Descripción |
|------------------|-------------|--------|--|--------|-------------|
| vg00 | root | 4GB | / | XFS | Root FS |
| | var | 45GB | /var | XFS | Var FS |
| | home | 2GB | /home | XFS | |
| | tmp | 2GB | /tmp | XFS | |
| | usr | 7GB | /usr | XFS | |
| | opt | 5GB | /opt | XFS | |
| | openv | 5GB | /usr/openv | XFS | |
| | swap | 8GB | swap | [SWAP] | Swap |
| docker-vg | docker-pool | [todo] | N/A | - | Docker |
| logging-vg ** | logging-es | 300GB | /usr/local/logging-es uid:1000,gid:1000 | XFS | Logging |

** Sólo para los Nodos Infra

NOTA

Tanto el VG como el LV de **docker** será creado por el script docker-storage-setup mencionado en las próximas secciones.

Bastión - Configuración general

A continuación se describe la configuración general de la máquina que actuará de servidor de instalación

Información general

| | |
|-------------------|-------------------------------------|
| Root Password | root00 |
| Sistema Operativo | Red Hat Enterprise Linux 7.5 x86_64 |
| Firewall | Enabled |
| SELinux | Enforcing |
| Lang | en_US.UTF-8 |
| Keyboard | US |
| Timezone | America/Argentina/Buenos Aires |
| Packages | Base |

Particionado de disco SO y configuración LVM

| Partición | Tamaño | Mount | FS | Descripción |
|-----------|---------|------------|-----|-------------|
| 1 | 1024 MB | /boot | XFS | Boot FS |
| 2 | [Resto] | [LVM vg00] | - | LVM |

| VG | LV | Size | Mount | FS | Descripción |
|------|-------|------|------------|--------|-------------|
| vg00 | root | 4GB | / | XFS | Root FS |
| | var | 45GB | /var | XFS | Var FS |
| | home | 2GB | /home | XFS | |
| | tmp | 2GB | /tmp | XFS | |
| | usr | 7GB | /usr | XFS | |
| | opt | 5GB | /opt | XFS | |
| | openv | 5GB | /usr/openv | XFS | |
| | swap | 8GB | swap | [SWAP] | Swap |

Storage Persistente

Detalle de los volúmenes persistentes necesarios:

| Nombre | Entorno | Cant. | Tipo | Share | Descripción | Tamaño | Endpoint |
|-------------------------|---------|-------|---------|-------------------------------|--|--------|-------------|
| Registry | PROD | 1 | NFS | /OSEPREGISTRY_p_openshift_apu | Registry donde se guardarán las imágenes de Docker | 300GB | 10.92.49.14 |
| | noPROD | 1 | NFS | /OSENREGISTRY_d_openshift_apu | | 300GB | 10.92.49.14 |
| Logging | Ambos | 3 | vm-disk | Montado local en los nodos | Volúmen para los logs de los Containers | 300GB | N/A |
| Metrics | PROD | 1 | NFS | /OSEPMETRICS_p_openshift_apu | Volúmen para las métricas | 300GB | 10.92.49.14 |
| | noPROD | 1 | NFS | /OSENMETRICS_d_openshift_apu | | 300GB | 10.92.49.14 |
| Service Catalog | PROD | 1 | NFS | /OSEPCATALOG_p_openshift_apu | Volúmen para el service catalog | 5GB | 10.92.49.14 |
| | noPROD | 1 | NFS | /OSENACATALOG_d_openshift_apu | | 5GB | 10.92.49.14 |
| Cloudforms Bkp | Ambos | 1 | NFS | /CFMEBKP_p_openshift_apu | Volúmen para backup de Cloudforms | 100GB | 10.92.49.14 |
| Cloudforms Support Data | Ambos | 1 | NFS | /CFMESUPDAT_p_openshift_apu | Volúmen para Support Data de Cloudforms | 10GB | 10.92.49.14 |

Los volúmenes NFS serán presentados por un Storage NAS del Cliente. El acceso desde la red de Servidores debe estar habilitado. Los Shares NFS deben permitir acceder con todos los privilegios y permitir que cualquier ID de usuario pueda leer, escribir y ejecutar..

Certificados SSL

Se utilizarán certificados autofirmados durante todo el proceso de implementación

Se detalla a continuación la configuración necesaria para extender el tiempo de expiración de los mismos:

Dentro del `inventory_ocp_install` agregar

```
...
openshift_hosted_registry_cert_expire_days=3650
openshift_node_cert_expire_days=3650
openshift_master_cert_expire_days=3650
etcd_ca_default_days=1825
openshift_ca_cert_expire_days=1825
...
```

Autenticación de usuarios

La autenticación de usuarios será centralizada en un directorio del tipo LDAP.

Se utilizará la siguiente información para su configuración:

- Usuario y password para realizar consultas en el LDAP
 - bindDN = CN=Openshift AD,OU=Servicios,OU=Usuarios de CTI,DC=ctimovil,DC=net
 - bindPassword = *****
- FQDN: ldap.claro.amx
- Puerto: 389
- Protocolo: ldap
- CA certificate: N/A
- Insecure: true
- Base DN: DC=ctimovil,DC=net
- Grupos:
 - PROD:
 - osep01-Openshift
 - osep01-Admin
 - osep01-Admin-Project
 - osep01-Dev
 - noPROD:
 - osen01-Openshift
 - osen01-Admin-Project
 - osen01-Admin
 - osen01-Dev
- User Identifier: sAMAccountName

DNS y Balanceo de carga

Para la instalación de la plataforma OpenShift Container Platform es necesario tener una correcta resolución de nombres. Debemos asegurarnos de que cada host que participe del esquema a instalar pueda resolver el nombre de cualquiera de los demás hosts, tanto de los nodos como de los masters.

Además de los nombres de los servidores también se dieron de alta en DNS y se configuraron a nivel Balanceo F5:

Balanceo PROD:

| FQDN | F5 VIP | Port | Real Servers | SSL/TLS |
|-----------------------------|--------------|------|---|-------------|
| osep01-api.claro.amx | 10.92.55.191 | 443 | 10.92.84.80 10.92.84.81 10.92.84.82 | Passthrough |
| osep01-api-int.claro.amx | 10.92.55.192 | 443 | 10.92.84.80 10.92.84.81 10.92.84.82 | Passthrough |
| *.osep01-apps.claro.amx | 10.92.55.189 | 443 | 10.92.84.83 10.92.84.84 10.92.84.85 | Edge |
| *.osep01-apps-ssl.claro.amx | 10.92.55.190 | 443 | 10.92.84.83 10.92.84.84 10.92.84.85 | Passthrough |

Balanceo noPROD:

| FQDN | F5 VIP | Port | Real Servers | SSL/TLS |
|-----------------------------|---------------|------|---|-------------|
| osen01-api.claro.amx | 10.105.218.69 | 443 | 10.92.84.90 10.92.84.91 10.92.84.92 | Passthrough |
| osen01-api-int.claro.amx | 10.105.218.70 | 443 | 10.92.84.90 10.92.84.91 10.92.84.92 | Passthrough |
| *.osen01-apps.claro.amx | 10.105.218.67 | 443 | 10.92.84.93 10.92.84.94 10.92.84.95 | Edge |
| *.osen01-apps-ssl.claro.amx | 10.105.218.68 | 443 | 10.92.84.93 10.92.84.94 10.92.84.95 | Passthrough |

INSTALACIÓN

Lineamientos generales de la instalación

Plan de Acción (POA)

El siguiente es el plan de acción para la implementación del ambiente de Openshift

- Preparación de los servidores
- Instalación de Openshift
- Ejecución de tareas post-instalación

Preparación de los servidores

Listado de tareas previas a la instalación de Openshift

Suscripciones y repositorios

Repositorios

Es necesario suscribir los servidores a los siguientes repositorios:

- rhel-7-server-extras-rpms
- rhel-7-server-rpms
- rhel-7-server-ose-3.9-rpms
- rhel-7-fast-datapath-rpms
- rhel-7-server-ansible-2.4-rpms

NOTA

Se utilizará el servidor Bastión como repositorio centralizado de RPMs para la instalación siguiendo los lineamientos de la modalidad de instalación “Disconnected”

https://docs.openshift.com/container-platform/3.9/install_config/install/disconnected_install.html

Acceso a los servidores

Se realizará un cruce de claves SSH entre el Bastión y el resto de los servidores, utilizando el usuario root.

Ansible utiliza protocolo SSH para ejecutar las tareas incluídas en los playbooks. A modo de ejemplo se listan a continuación las configuraciones necesarias:

Generación de par de claves en servidor origen:

```
# ssh-keygen
```

IMPORTANTE

No especificar una password para la clave SSH a generar

Luego debemos distribuir dicha clave en todos los hosts involucrados en la instalación, por ejemplo:

```
# for host in master.example.com node1.example.com
do
    ssh-copy-id -i ~/.ssh/id_rsa.pub $host
done
```

** Modificar los hostnames del comando según el caso*

Instalación de paquetes RPM

Ejecutar en todos los servidores

```
yum install wget git net-tools bind-utils yum-utils iptables-services
bridge-utils bash-completion kexec-tools sos psacct

yum update

yum install atomic-openshift-utils

yum install docker-1.13.1

reboot
```

Docker Storage

Los imágenes y contenedores Docker se almacenarán localmente en cada servidor dentro del Docker Storage.

Se necesita crear en todos los servidores el archivo `/etc/sysconfig/docker-storage-setup`, y debe contener el nombre del VG y el disco que se utilizará como PV.

```
cat /etc/sysconfig/docker-storage-setup  
DEVS=/dev/sdb  
VG=docker-vg
```

Para configurarlo ejecutar el comando:

```
docker-storage-setup
```

Reiniciar el servicio de Docker

```
systemctl restart docker  
systemctl enable docker  
systemctl is-active docker
```

Openshift Deploy

Para el deploy de Openshift se utilizan Playbooks de Ansible y se ejecutaron las siguiente tareas en el servidor Bastión:

Armado de Inventory File

Ansible necesita un archivo de inventario de servidores `inventory_ocp_install(*)` para identificar qué tareas y dónde debe ejecutarlas.

Contiene toda la parametrización de la instalación, incluyendo integración con Identity Providers externos y persistencia de datos en storage externo, entre otros.

** Ver en el ANEXO el contenido del Ansible `inventory_ocp_install`*

Instalación de Openshift

A partir de la versión OCP v3.9 se dividió la instalación en dos playbooks principales. El primero configura y valida todos los prerequisites incluidos en el Inventory File

```
# ansible-playbook -f 20 -i /root/CLARO/[Prod,noProd]/inventory_ocp_install \
/usr/share/ansible/openshift-ansible/playbooks/prerequisites.yaml
```

El segundo instala y configura la plataforma Openshift

```
# ansible-playbook -f 20 -i /root/CLARO/[Prod,noProd]/inventory_ocp_install \
/usr/share/ansible/openshift-ansible/playbooks/deploy_cluster.yaml
```

Tareas post-instalación

Detalle de las tareas post-instalación:

- Privilegios de administración del cluster
- Integración con Cloudforms

Tareas post-cluster-deploy

Nos conectaremos un Master y ejecutaremos

```
* Conectarse al proyecto
# oc project logging

* Deshabilitar para que los pod de fluentd no se ejecuten en los master
* Para Prod:
  oc label node osep01-master-01.claro.amx --overwrite logging-infra-fluentd=false
  oc label node osep01-master-02.claro.amx --overwrite logging-infra-fluentd=false
  oc label node osep01-master-03.claro.amx --overwrite logging-infra-fluentd=false
* Para noProd:
  oc label node osen01-master-01.claro.amx --overwrite logging-infra-fluentd=false
  oc label node osen01-master-02.claro.amx --overwrite logging-infra-fluentd=false
  oc label node osen01-master-03.claro.amx --overwrite logging-infra-fluentd=false

* Configuración del volumen persistente para Elasticsearch
# oadm policy add-scc-to-user privileged \
system:serviceaccount:logging:aggregated-logging-elasticsearch

for dc in $(oc get deploymentconfig --selector component=es -o name)
do
  oc scale $dc --replicas=0
  oc patch $dc -p '{"spec":{"template":{"spec":{"containers":[{"name":"elasticsearch","securityContext":{"privileged": true}}]}}}}'
done

*Cada instancia de Elasticsearch debe estar asignada a un nodo de infra
Ej: oc patch dc/logging-es-data-master-<suffix> -p '{"spec":{"template":{"spec":{"nodeSelector":{"nodenumber":"<nro del
nodo>"}}}}}'

for dc in $(oc get deploymentconfig --selector logging-infra=elasticsearch -o name)
do
  oc set volume $dc --add --overwrite --name=elasticsearch-storage --type=hostPath --path=/usr/local/logging-es
  oc rollout latest $dc
  oc scale $dc --replicas=1
done
```


Privilegios administración del cluster

Asignación de privilegios de administración del cluster al usuario LOCAL:admin

```
oc adm policy add-cluster-role-to-user cluster-admin admin
```

Integración con Cloudforms

Configurar Capacity & Utilization

Para que funcione la recolección de métricas será necesario habilitar tres roles:

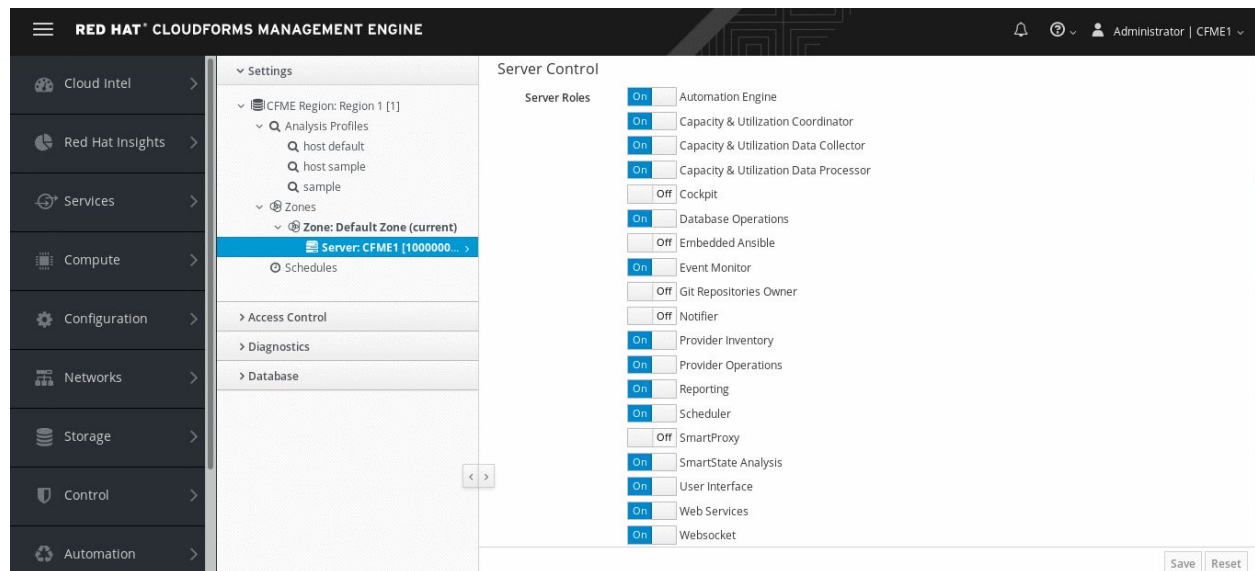
1. Desde el menú Settings, seleccionar Configuration, luego seleccionar el Server desde Settings → Zone a la izquierda.
2. Configurar el Company Name, Appliance Name, Appliance Time Zone.
3. Buscar el listado de Server Roles y configurar en ON:
 1. Capacity & Utilization Coordinator
 2. Capacity & Utilization Data Collector
 3. Capacity & Utilization Data Processor
4. Click Save

Habilitar Smartstate Analysis

Luego de habilitar los roles hay que habilitar el SmartState analysis.

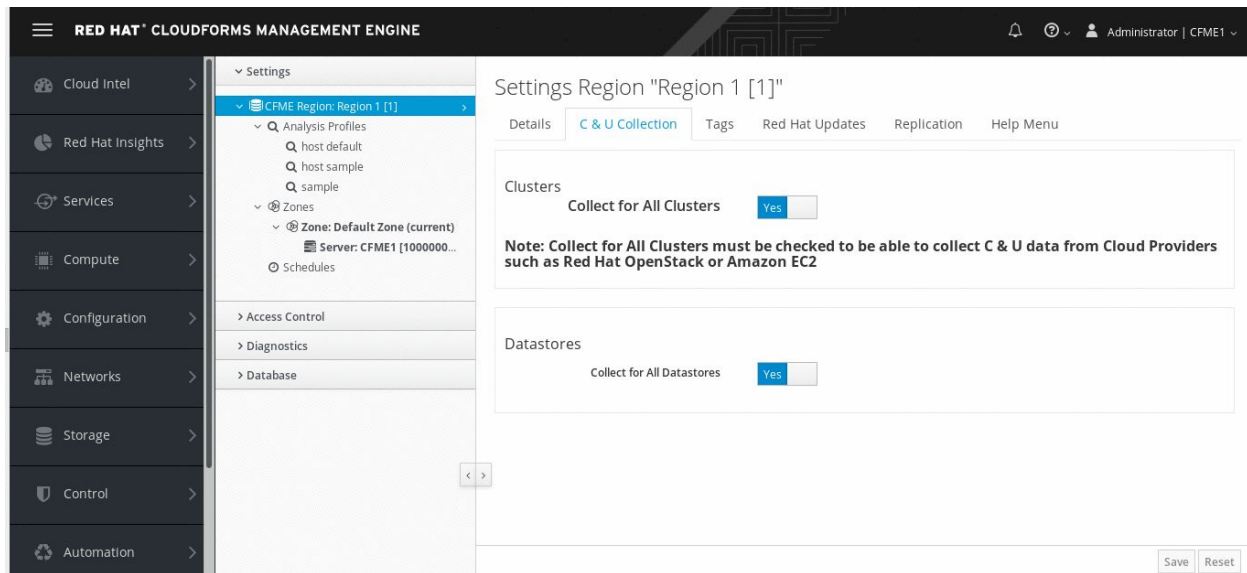
Es similar al procedimiento anterior, salvo que hay que poner en ON otros roles, a saber:

1. SmartProxy
2. SmartState Analysis
3. Salvar la configuración



También es necesario habilitar C&U a nivel de Región:

En Configuration, pararse sobre la Región y luego en la solapa “C & U Collection” habilitar tanto para Clusters y Datastores



Alta del Container Provider

Para integrar Openshift a Cloudforms se obtendrá el token de management-admin

Nos conectaremos a a un servidor Master:

```
oc sa get-token -n management-infra management-admin
```

En CloudForms web console:

- Pararse sobre “Compute” en el menú de la izquierda, luego “Containers” y por último “Providers”.
- Seleccionar el botón “Configuration” y luego “Add a New Containers Provider”.
- Ingresar el nombre del provider y seleccionar tipo Openshift Container Platform
- Dentro de “Endpoints”, en la solapa Default, ingresar la dirección del OpenShift Master API en “Hostname” y pegar el token obtenido anteriormente dentro de “Token” y “Confirm Token”. Click en Validate para verificar la conectividad
- Dentro de “Endpoints”, seleccionar la solapa “Hawkular” e ingresar el hawkular-metrics hostname en el campo Hostname
- Por último click en “Add” para finalizar

RED HAT® CLOUDFORMS MANAGEMENT ENGINE

Containers Providers > OCP-PROD (Dashboard) > Edit Containers Providers 'OCP-PROD'

Name:

Type:

Zone:

Alerts:

Metrics:

Endpoints

Default Metrics

Security Protocol:

Hostname (or IPv4 or IPv6 address):

API Port:

Token: [Change stored token](#)

RED HAT® CLOUDFORMS MANAGEMENT ENGINE

Containers Providers > OCP-PROD (Dashboard) > Edit Containers Providers 'OCP-PROD'

Name:

Type:

Zone:

Alerts:

Metrics:

Endpoints

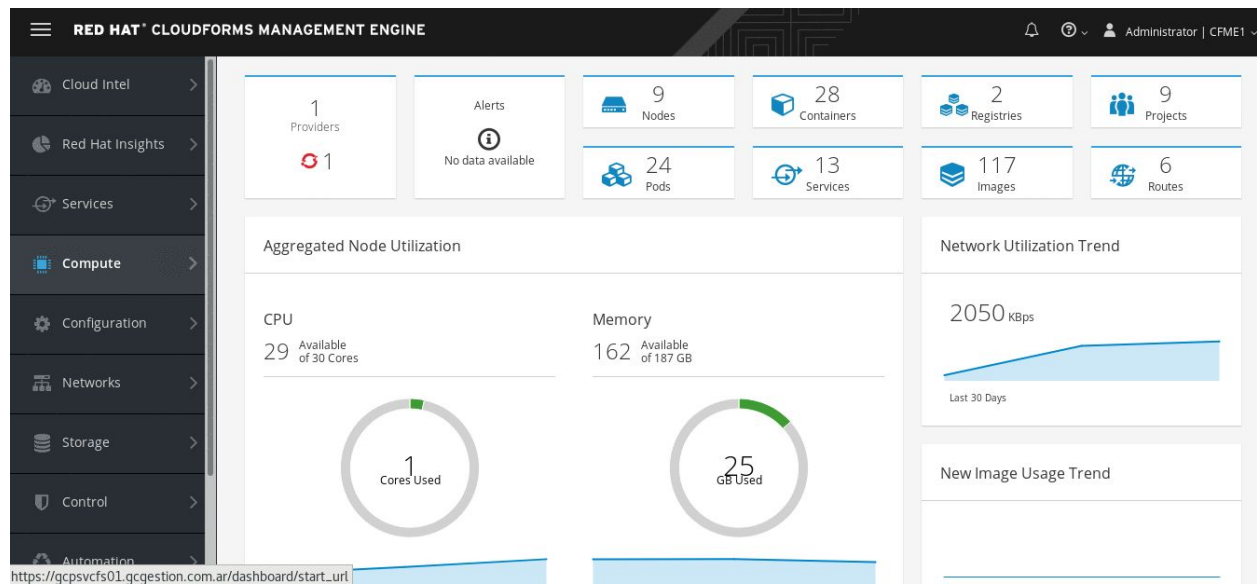
Default Metrics

Security Protocol:

Hostname (or IPv4 or IPv6 address):

API Port:

Openshift Summary



Logcollector y Backup

- Ir a Administrator (menu arriba esquina sup izquierda) ---> Configuration
 - Elegir la solapa vertical "Diagnostics" (Hay 4, Settings/AccessControl/Diagnostics/Database)
 - Elegir la solapa horizontal "Collect Logs"
 - Oprimir el boton "Edit" (arriba)
 - Completar los datos:
 - * type: nfs
 - * depot name: CFME-SUPDAT
 - * uri: [NFS_SERVER_HOSTNAME]/exports/cfme-supdat
 - Oprimir Save
 - Probarlo con el botón "Collect".
-
- Ir a Administrator (menu arriba esquina sup izquierda) ---> Configuration
 - Elegir la solapa vertical "Settings" (Hay 4, Settings/AccessControl/Diagnostics/Database)
 - Ubicar el elemento "schedules", dentro de la "CFME Region".
 - Oprimir el boton "configuration" ---> "add new schedule"
 - Elegir el Type "dababase backup".

ANEXO A - ANSIBLE FILES

Inventory_ocp_install para PROD:

```
[OSEv3:children]
masters
nodes
etcd

[OSEv3:vars]
ansible_ssh_user=root
openshift_deployment_type=openshift-enterprise
openshift_enable_unsupported_configurations=True
openshift_docker_insecure_registries=10.92.240.0/21
openshift_docker_blocked_registries=docker.io
openshift_docker_options="--log-driver json-file --log-opt max-size=1M --log-opt max-file=3"

openshift_hosted_registry_cert_expire_days=3650
openshift_node_cert_expire_days=3650
openshift_master_cert_expire_days=3650
etcd_ca_default_days=1825
openshift_ca_cert_expire_days=1825

openshift_master_cluster_method=native
openshift_master_cluster_hostname=osep01-api-int.claro.amx
openshift_master_cluster_public_hostname=osep01-api.claro.amx

openshift_node_kubelet_args=('pods-per-core': ['100'], 'max-pods': ['250'], 'image-gc-high-threshold': ['90'],
'image-gc-low-threshold': ['80'])
openshift_clock_enabled=true

openshift_master_identity_providers=[{'name': 'LOCAL', 'login': 'true', 'challenge': 'true', 'kind':
'HTPasswdPasswordIdentityProvider', 'filename': '/etc/origin/master/htpasswd'}, {'name': 'CLARO AD', 'challenge':
'true', 'login': 'true', 'kind': 'LDAPPasswordIdentityProvider', 'attributes': {'id': ['cn'], 'email': ['mail'], 'name':
['displayName'], 'preferredUsername': ['sAMAccountName']}, 'bindDN': 'CN=Openshift
AD,OU=Servicios,OU=Usuarios de CTI,DC=ctimovil,DC=net', 'bindPassword': 'Claro2018', 'ca': '', 'insecure': 'true',
'url':
'ldap://ldap.claro.amx:389/DC=ctimovil,DC=net?sAMAccountName?sub?(memberOf=CN=osep01-Openshift,OU
=Acceso a servicios,OU=Grupos de CTI,DC=ctimovil,DC=net)'}]

openshift_master_htpasswd_file=/root/CLARO/htpasswd

openshift_master_default_subdomain=osep01-apps.claro.amx

# Router Selector
openshift_router_selector='region=infra'

# REGISTRY
openshift_registry_selector='region=infra'

openshift_hosted_registry_routehost=docker-registry-default.osep01-apps-ssl.claro.amx

openshift_hosted_registry_replicas=3
openshift_hosted_registry_storage_kind=nfs
openshift_hosted_registry_storage_access_modes=['ReadWriteMany']
```

```
openshift_hosted_registry_storage_host=nfs.claro.amx
openshift_hosted_registry_storage_nfs_directory=/OSEPREGISTRY_p_openshift_apu
openshift_hosted_registry_storage_volume_name=registry
openshift_hosted_registry_storage_volume_size=300Gi

# Configure the multi-tenant SDN plugin (default is 'redhat/openshift-ovs-subnet')
os_sdn_network_plugin_name='redhat/openshift-ovs-multitenant'

# Disable the OpenShift SDN plugin
# openshift_use_openshift_sdn=False

# Configure SDN cluster network CIDR block. This network block should
# be a private block and should not conflict with existing network
# blocks in your infrastructure that pods may require access to.
# Can not be changed after deployment.
osm_cluster_network_cidr=10.128.0.0/20
openshift_master_portal_net=10.92.240.0/21

# Configure number of bits to allocate to each host.s subnet e.g. 8
# would mean a /24 network on the host.
osm_host_subnet_length=8

openshift_master_api_port=443
openshift_master_console_port=443

openshift_master_session_name=ssn
openshift_master_session_max_seconds=3600

# Configure logrotate scripts
# See: https://github.com/nickhammond/ansible-logrotate
logrotate_scripts=[{"name": "syslog", "path":
"/var/log/cron\n/var/log/maillog\n/var/log/messages\n/var/log/secure\n/var/log/spooler\n", "options":
["daily", "rotate 7", "compress", "sharedscripts", "missingok"], "scripts": {"postrotate": "/bin/kill -HUP `cat
/var/run/syslogd.pid 2> /dev/null` 2> /dev/null || true"}}]

# METRICS

# Enable Cluster Metrics
openshift_metrics_install_metrics=true

# Cluster Metrics Storage
openshift_metrics_hawkular_nodeselector={"region":"infra"}
openshift_metrics_cassandra_nodeselector={"region":"infra"}
openshift_metrics_heapster_nodeselector={"region":"infra"}
openshift_metrics_hawkular_hostname=hawkular-metrics.osep01-apps-ssl.claro.amx

openshift_metrics_storage_kind=nfs
openshift_metrics_storage_access_modes=['ReadWriteOnce']
openshift_metrics_storage_host=nfs.claro.amx
openshift_metrics_storage_nfs_directory=/OSEPMETRICS_p_openshift_apu
openshift_metrics_storage_volume_name=metrics
openshift_metrics_storage_volume_size=300Gi

# LOGGING deployment

openshift_logging_namespace=logging
openshift_logging_install_logging=true
openshift_logging_curator_default_days=90
openshift_logging_kibana_hostname=kibana.osep01-apps-ssl.claro.amx
```

```
openshift_logging_kibana_replica_count=3
openshift_logging_kibana_nodeselector={"region":"infra"}
openshift_logging_fluentd_hosts=['--all']
openshift_logging_es_cluster_size=3
openshift_logging_es_nodeselector={"region":"infra"}
openshift_logging_curator_nodeselector={"region":"infra"}
openshift_logging_master_public_url=https://osep01-api.claro.amx
openshift_master_logging_public_url=https://kibana.osep01-apps-ssl.claro.amx

#SERVICE CATALOG
openshift_enable_service_catalog=true

openshift_hosted_etcd_storage_kind=nfs
openshift_hosted_etcd_storage_nfs_directory=/OSEPCATALOG_p_openshift_apu
openshift_hosted_etcd_storage_volume_name=etcd-vol2
openshift_hosted_etcd_storage_host=nfs.claro.amx
openshift_hosted_etcd_storage_access_modes=["ReadWriteOnce"]
openshift_hosted_etcd_storage_volume_size=5G
openshift_hosted_etcd_storage_labels={'storage': 'etcd'}

ansible_service_broker_local_registry_whitelist=['.*-apb$']

template_service_broker_selector={"region": "infra"}

[masters]
osep01-master-01.claro.amx
osep01-master-02.claro.amx
osep01-master-03.claro.amx

[etcd]
osep01-master-01.claro.amx
osep01-master-02.claro.amx
osep01-master-03.claro.amx

[nodes]
osep01-master-01.claro.amx openshift_ip=10.92.84.80 openshift_node_labels="{ 'region': 'master' }"
osep01-master-02.claro.amx openshift_ip=10.92.84.81 openshift_node_labels="{ 'region': 'master' }"
osep01-master-03.claro.amx openshift_ip=10.92.84.82 openshift_node_labels="{ 'region': 'master' }"
osep01-infra-01.claro.amx openshift_ip=10.92.84.83 openshift_node_labels="{ 'region':
'infra', 'node-role.kubernetes.io/infra': 'true', 'logging-es-node': '1' }"
osep01-infra-02.claro.amx openshift_ip=10.92.84.84 openshift_node_labels="{ 'region':
'infra', 'node-role.kubernetes.io/infra': 'true', 'logging-es-node': '2' }"
osep01-infra-03.claro.amx openshift_ip=10.92.84.85 openshift_node_labels="{ 'region':
'infra', 'node-role.kubernetes.io/infra': 'true', 'logging-es-node': '3' }"
osep01-worker-01.claro.amx openshift_ip=10.92.84.86 openshift_node_labels="{ 'region': 'apps' }"
osep01-worker-02.claro.amx openshift_ip=10.92.84.87 openshift_node_labels="{ 'region': 'apps' }"
osep01-worker-03.claro.amx openshift_ip=10.92.84.88 openshift_node_labels="{ 'region': 'apps' }"
osep01-worker-04.claro.amx openshift_ip=10.92.84.89 openshift_node_labels="{ 'region': 'apps' }"
```


Inventory_ocp_install para noPROD:

```
[OSEv3:children]
masters
nodes
etcd

[OSEv3:vars]
ansible_ssh_user=root
openshift_deployment_type=openshift-enterprise
openshift_enable_unsupported_configurations=True
openshift_docker_insecure_registries=10.92.248.0/21
openshift_docker_blocked_registries=docker.io
openshift_docker_options="--log-driver json-file --log-opt max-size=1M --log-opt max-file=3"

openshift_hosted_registry_cert_expire_days=3650
openshift_node_cert_expire_days=3650
openshift_master_cert_expire_days=3650
etcd_ca_default_days=1825
openshift_ca_cert_expire_days=1825

openshift_master_cluster_method=native
openshift_master_cluster_hostname=osen01-api-int.claro.amx
openshift_master_cluster_public_hostname=osen01-api.claro.amx

openshift_node_kubelet_args=('pods-per-core': ['100'], 'max-pods': ['250'], 'image-gc-high-threshold': ['90'],
'image-gc-low-threshold': ['80'])
openshift_clock_enabled=true

openshift_master_identity_providers=[{'name': 'LOCAL', 'login': 'true', 'challenge': 'true', 'kind':
'HTPasswdPasswordIdentityProvider', 'filename': '/etc/origin/master/htpasswd'}, {'name': 'CLARO AD', 'challenge':
'true', 'login': 'true', 'kind': 'LDAPPasswordIdentityProvider', 'attributes': {'id': ['cn'], 'email': ['mail'], 'name':
['displayName'], 'preferredUsername': ['sAMAccountName']}, 'bindDN': 'CN=Openshift
AD,OU=Servicios,OU=Usuarios de CTI,DC=ctimovil,DC=net', 'bindPassword': 'Claro2018', 'ca': '', 'insecure': 'true',
'url':
'ldap://ldap.claro.amx:389/DC=ctimovil,DC=net?sAMAccountName?sub?(memberOf=CN=osep01-Openshift,OU
=Acceso a servicios,OU=Grupos de CTI,DC=ctimovil,DC=net)'}]

openshift_master_htpasswd_file=/root/CLARO/htpasswd

openshift_master_default_subdomain=osen01-apps.claro.amx

# Router Selector
openshift_router_selector='region=infra'

# REGISTRY
openshift_registry_selector='region=infra'

openshift_hosted_registry_routehost=docker-registry-default.osen01-apps-ssl.claro.amx

openshift_hosted_registry_replicas=3
openshift_hosted_registry_storage_kind=nfs
openshift_hosted_registry_storage_access_modes=['ReadWriteMany']
openshift_hosted_registry_storage_host=nfs.claro.amx
openshift_hosted_registry_storage_nfs_directory=/OSENREGISTRY_d_openshift_apu
openshift_hosted_registry_storage_volume_name=registry
openshift_hosted_registry_storage_volume_size=300Gi
```

```
# Configure the multi-tenant SDN plugin (default is 'redhat/openshift-ovs-subnet')
os_sdn_network_plugin_name='redhat/openshift-ovs-multitenant'

# Disable the OpenShift SDN plugin
# openshift_use_openshift_sdn=False

# Configure SDN cluster network CIDR block. This network block should
# be a private block and should not conflict with existing network
# blocks in your infrastructure that pods may require access to.
# Can not be changed after deployment.
osm_cluster_network_cidr=10.129.0.0/20
openshift_master_portal_net=10.92.248.0/21

# Configure number of bits to allocate to each host.s subnet e.g. 8
# would mean a /24 network on the host.
osm_host_subnet_length=8

openshift_master_api_port=443
openshift_master_console_port=443

openshift_master_session_name=ssn
openshift_master_session_max_seconds=3600

# Configure logrotate scripts
# See: https://github.com/nickhammond/ansible-logrotate
logrotate_scripts=[{"name": "syslog", "path":
"/var/log/cron\n/var/log/maillog\n/var/log/messages\n/var/log/secure\n/var/log/spooler\n", "options":
["daily", "rotate 7", "compress", "sharedscripts", "missingok"], "scripts": {"postrotate": "/bin/kill -HUP `cat
/var/run/syslogd.pid 2> /dev/null` 2> /dev/null || true"}}]

# METRICS

# Enable Cluster Metrics
openshift_metrics_install_metrics=true

# Cluster Metrics Storage
openshift_metrics_hawkular_nodeselector={"region":"infra"}
openshift_metrics_cassandra_nodeselector={"region":"infra"}
openshift_metrics_heapster_nodeselector={"region":"infra"}
openshift_metrics_hawkular_hostname=hawkular-metrics.osen01-apps-ssl.claro.amx

openshift_metrics_storage_kind=nfs
openshift_metrics_storage_access_modes=['ReadWriteOnce']
openshift_metrics_storage_host=nfs.claro.amx
openshift_metrics_storage_nfs_directory=/OSENMETRICS_d_openshift_apu
openshift_metrics_storage_volume_name=metrics
openshift_metrics_storage_volume_size=300Gi

# LOGGING deployment

openshift_logging_namespace=logging
openshift_logging_install_logging=true
openshift_logging_curator_default_days=90
openshift_logging_kibana_hostname=kibana.osen01-apps-ssl.claro.amx
openshift_logging_kibana_replica_count=3
openshift_logging_kibana_nodeselector={"region":"infra"}
openshift_logging_fluentd_hosts=['--all']
openshift_logging_es_cluster_size=3
openshift_logging_es_nodeselector={"region":"infra"}
```

```
openshift_logging_curator_nodeselector={"region":"infra"}
openshift_logging_master_public_url=https://osen01-api.claro.amx
openshift_master_logging_public_url=https://kibana.osen01-apps-ssl.claro.amx

#SERVICE CATALOG
openshift_enable_service_catalog=true

openshift_hosted_etcd_storage_kind=nfs
openshift_hosted_etcd_storage_nfs_directory=/OSEN_CATALOG_td_openshift_apu
openshift_hosted_etcd_storage_volume_name=etcd-vol2
openshift_hosted_etcd_storage_host=nfs.claro.amx
openshift_hosted_etcd_storage_access_modes=["ReadWriteOnce"]
openshift_hosted_etcd_storage_volume_size=5G
openshift_hosted_etcd_storage_labels={'storage': 'etcd'}

ansible_service_broker_local_registry_whitelist=['.*-apb$']

template_service_broker_selector={"region": "infra"}

[masters]
osen01-master-01.claro.amx
osen01-master-02.claro.amx
osen01-master-03.claro.amx

[etcd]
osen01-master-01.claro.amx
osen01-master-02.claro.amx
osen01-master-03.claro.amx

[nodes]
osen01-master-01.claro.amx openshift_ip=10.92.84.90 openshift_node_labels="{ 'region': 'master' }"
osen01-master-02.claro.amx openshift_ip=10.92.84.91 openshift_node_labels="{ 'region': 'master' }"
osen01-master-03.claro.amx openshift_ip=10.92.84.92 openshift_node_labels="{ 'region': 'master' }"
osen01-infra-01.claro.amx openshift_ip=10.92.84.93 openshift_node_labels="{ 'region': 'infra', 'node-role.kubernetes.io/infra': 'true', 'logging-es-node': '1' }"
osen01-infra-02.claro.amx openshift_ip=10.92.84.94 openshift_node_labels="{ 'region': 'infra', 'node-role.kubernetes.io/infra': 'true', 'logging-es-node': '2' }"
osen01-infra-03.claro.amx openshift_ip=10.92.84.95 openshift_node_labels="{ 'region': 'infra', 'node-role.kubernetes.io/infra': 'true', 'logging-es-node': '3' }"
osen01-worker-01.claro.amx openshift_ip=10.92.84.96 openshift_node_labels="{ 'region': 'apps' }"
osen01-worker-02.claro.amx openshift_ip=10.92.84.97 openshift_node_labels="{ 'region': 'apps' }"
osen01-worker-03.claro.amx openshift_ip=10.92.84.98 openshift_node_labels="{ 'region': 'apps' }"
osen01-worker-04.claro.amx openshift_ip=10.92.84.99 openshift_node_labels="{ 'region': 'apps' }"
```

CONTROL DEL DOCUMENTO

Contribuidores

| Nombre | Datos de Contacto |
|------------------|----------------------|
| Luis P. Aparicio | laparicio@redhat.com |
| | |
| | |

Revisiones

| Version | Autor | Comentario | Fecha |
|---------|------------------|-------------------|------------|
| 1.0 | Luis P. Aparicio | Documento Inicial | 2-JUL-2018 |
| | | | |
| | | | |
| | | | |