



Opciones de configuración avanzadas

NetApp Solutions

NetApp
December 19, 2024

Tabla de contenidos

- Opciones de configuración avanzadas 1
 - Exploración de las opciones de equilibrio de carga 1
 - Creación de registros privados de imágenes 22

Opciones de configuración avanzadas

Exploración de las opciones de equilibrio de carga

Análisis de las opciones de equilibrador de carga: Red Hat OpenShift con NetApp

En la mayoría de los casos, Red Hat OpenShift hace que las aplicaciones estén disponibles para el mundo exterior a través de rutas. Un servicio es expuesto dándole un nombre de host accesible desde el exterior. Un enrutador OpenShift puede consumir la ruta definida y los puntos finales identificados por su servicio para proporcionar esta conectividad con nombre a clientes externos.

Sin embargo, en algunos casos, las aplicaciones requieren la puesta en marcha y configuración de equilibradores de carga personalizados para exponer los servicios adecuados. Un ejemplo de esto es Astra Control Center de NetApp. Para satisfacer esta necesidad, hemos evaluado una serie de opciones de equilibrador de carga personalizadas. Su instalación y configuración se describen en esta sección.

En las siguientes páginas se ofrece información adicional sobre las opciones de equilibrador de carga validadas en la solución Red Hat OpenShift con NetApp:

- ["MetalLB"](#)
- ["BIG-IP DE F5"](#)

Instalación de equilibradores de carga de MetalLB: Red Hat OpenShift con NetApp

En esta página se enumeran las instrucciones de instalación y configuración del equilibrador de carga de MetalLB.

MetalLB es un equilibrador de carga de red autoalojado instalado en el clúster de OpenShift que permite la creación de servicios OpenShift de equilibrador de carga de tipo en clústeres que no se ejecutan en un proveedor de cloud. Las dos principales características de MetalLB que trabajan conjuntamente para apoyar los servicios LoadBalancer son la asignación de direcciones y el anuncio externo.

Opciones de configuración de MetalLB

Basándose en cómo MetalLB anuncia la dirección IP asignada a los servicios LoadBalancer fuera del clúster OpenShift, funciona en dos modos:

- **Modo de capa 2.** en este modo, un nodo del clúster OpenShift asume la propiedad del servicio y responde a las solicitudes ARP de esa IP para hacerla accesible fuera del clúster OpenShift. Como solo el nodo anuncia la IP, presenta un cuello de botella de ancho de banda y unas limitaciones lentas de conmutación al respaldo. Para obtener más información, consulte la documentación ["aquí"](#).
- **Modo BGP.** en este modo, todos los nodos del clúster OpenShift establecen sesiones de BGP peering con un router y anuncian las rutas para reenviar tráfico a las IP de servicio. El requisito previo para ello es integrar MetalLB con un router en esa red. Debido al mecanismo de hash en BGP, tiene ciertas limitaciones cuando cambia la asignación de IP a nodo para un servicio. Para obtener más información, consulte la documentación ["aquí"](#).



A efectos de este documento, configuraremos MetalLB en modo capa-2.

Instalación del equilibrador de carga de MetalLB

1. Descargar los recursos de MetalLB.

```
[netapp-user@rhel7 ~]$ wget
https://raw.githubusercontent.com/metallb/metallb/v0.10.2/manifests/namespace.yaml
[netapp-user@rhel7 ~]$ wget
https://raw.githubusercontent.com/metallb/metallb/v0.10.2/manifests/metallb.yaml
```

2. Editar archivo `metallb.yaml` y retirar `spec.template.spec.securityContext` Desde el despliegue del controlador y el altavoz `DemonSet`.

Líneas a borrar:

```
securityContext:
  runAsNonRoot: true
  runAsUser: 65534
```

3. Cree el `metallb-system` espacio de nombres.

```
[netapp-user@rhel7 ~]$ oc create -f namespace.yaml
namespace/metallb-system created
```

4. Cree el MetalLB CR.

```
[netapp-user@rhel7 ~]$ oc create -f metallb.yaml
podsecuritypolicy.policy/controller created
podsecuritypolicy.policy/speaker created
serviceaccount/controller created
serviceaccount/speaker created
clusterrole.rbac.authorization.k8s.io/metallb-system:controller created
clusterrole.rbac.authorization.k8s.io/metallb-system:speaker created
role.rbac.authorization.k8s.io/config-watcher created
role.rbac.authorization.k8s.io/pod-lister created
role.rbac.authorization.k8s.io/controller created
clusterrolebinding.rbac.authorization.k8s.io/metallb-system:controller
created
clusterrolebinding.rbac.authorization.k8s.io/metallb-system:speaker
created
rolebinding.rbac.authorization.k8s.io/config-watcher created
rolebinding.rbac.authorization.k8s.io/pod-lister created
rolebinding.rbac.authorization.k8s.io/controller created
daemonset.apps/speaker created
deployment.apps/controller created
```

5. Antes de configurar el altavoz MetalLB, conceda privilegios elevados DemonSet de altavoz para que pueda realizar la configuración de red necesaria para que los equilibradores de carga funcionen.

```
[netapp-user@rhel7 ~]$ oc adm policy add-scc-to-user privileged -n
metallb-system -z speaker
clusterrole.rbac.authorization.k8s.io/system:openshift:scc:privileged
added: "speaker"
```

6. Configure MetalLB creando un ConfigMap en la metallb-system espacio de nombres.

```
[netapp-user@rhel7 ~]$ vim metallb-config.yaml

apiVersion: v1
kind: ConfigMap
metadata:
  namespace: metallb-system
  name: config
data:
  config: |
    address-pools:
    - name: default
      protocol: layer2
      addresses:
      - 10.63.17.10-10.63.17.200

[netapp-user@rhel7 ~]$ oc create -f metallb-config.yaml
configmap/config created
```

7. Ahora, cuando se crean servicios loadbalancer, MetalLB asigna una IP externa a los servicios y anuncia la dirección IP respondiendo a las solicitudes ARP.



Si desea configurar MetalLB en modo BGP, omita el paso 6 anterior y siga el procedimiento descrito en la documentación de MetalLB ["aquí"](#).

Instalación de equilibradores de carga BIG-IP de F5

Big-IP de F5 es un controlador de entrega de aplicaciones (ADC) que ofrece un amplio conjunto de servicios avanzados de seguridad y gestión del tráfico de nivel de producción como el equilibrio de carga L4-L7, descarga SSL/TLS, DNS, firewall y muchos más. Estos servicios aumentan significativamente la disponibilidad, la seguridad y el rendimiento de sus aplicaciones.

Big-IP de F5 se puede implementar y consumir de varias maneras, en hardware dedicado, en la nube o como un dispositivo virtual en las instalaciones. Consulte la documentación [aquí](#) para explorar e implementar BIG-IP de F5 según sus necesidades.

Para una integración eficaz de los servicios BIG-IP de F5 con Red Hat OpenShift, F5 ofrece EL BIG-IP Container Ingress Service (CIS). CIS se instala como un controlador que supervisa la API de OpenShift para determinadas definiciones de recursos personalizados (CRD) y gestiona la configuración del sistema BIG-IP de F5. Big-IP CIS de F5 se puede configurar para controlar tipos de servicios LoadBalancers y rutas en OpenShift.

Además, para la asignación automática de direcciones IP para dar servicio al tipo LoadBalancer, puede utilizar el controlador F5 IPAM. El controlador IPAM de F5 se instala como un pod de controladores que mira la API de OpenShift para los servicios LoadBalancer con una anotación ipamLabel para asignar la dirección IP desde un grupo preconfigurado.

En esta página se enumeran las instrucciones de instalación y configuración del controlador F5 BIG-IP CIS e

IPAM. Como requisito previo, debe tener un sistema BIG-IP de F5 implementado y con licencia. También debe tener licencia para los servicios SDN, que se incluyen de forma predeterminada con la licencia base BIG-IP ve.



BIG-IP de F5 se puede implementar en modo independiente o en modo cluster. A efectos de esta validación, F5 BIG-IP se implementó en modo independiente, pero, a efectos de producción, es preferible disponer de un cluster de BIG-IP para evitar un único punto de fallo.



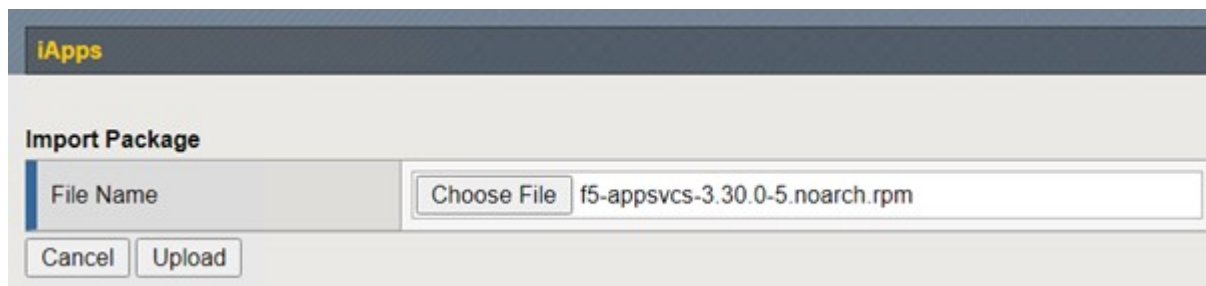
Un sistema BIG-IP de F5 se puede implementar en hardware dedicado, en la nube o como un dispositivo virtual en las instalaciones con versiones superiores a 12.x para que se integre con F5 CIS. A efectos de este documento, el sistema BIG-IP de F5 se validó como dispositivo virtual, por ejemplo, mediante LA edición BIG-IP ve.

Versiones validadas

Tecnología	Versión de software
Red Hat OpenShift	4.6 EUS, 4.7
EDICIÓN F5 BIG-IP VE	16.1.0
Servicio de entrada de contenedores F5	2.5.1
Controlador IPAM F5	0.1.4
F5 AS3	3.30.0

Instalación

1. Instale la extensión F5 Application Services 3 para permitir que los sistemas BIG-IP acepten configuraciones en JSON en lugar de comandos de imperativo. Vaya a. "[Repositorio de F5 AS3 GitHub](#)" y descargue el último archivo RPM.
2. Inicie sesión en el sistema BIG-IP de F5, desplácese a iApps > Package Management LX y haga clic en Import.
3. Haga clic en elegir archivo y seleccione el archivo de RPM AS3 descargado, haga clic en Aceptar y, a continuación, haga clic en cargar.



4. Confirme que la extensión AS3 se ha instalado correctamente.



5. A continuación, configure los recursos necesarios para la comunicación entre los sistemas OpenShift Y BIG-IP. En primer lugar, cree un túnel entre OpenShift y EL servidor BIG-IP creando una interfaz de túnel VXLAN en EL sistema BIG-IP para OpenShift SDN. Desplácese a Red > túneles > Perfiles, haga clic en Crear y establezca el perfil principal en vxlan y el tipo de inundación en multidifusión. Introduzca un nombre para el perfil y haga clic en terminado.

Network >> Tunnels : Profiles : VXLAN >> New VXLAN Profile...

General Properties

Name	vxlan-multipoint
Parent Profile	vxlan
Description	

Settings Custom

Port	4789
Flooding Type	Multicast <input checked="" type="checkbox"/>

Cancel Repeat Finished

6. Desplácese a Red > túneles > Lista de túneles, haga clic en Crear e introduzca el nombre y la dirección IP local del túnel. Seleccione el perfil de túnel que se creó en el paso anterior y haga clic en finalizado.

Network >> Tunnels : Tunnel List >> New Tunnel...

Configuration

Name	openshift_vxlan
Description	
Key	0
Profile	vxlan-multipoint
Local Address	10.63.172.239
Secondary Address	Any
Remote Address	Any
Mode	Bidirectional
MTU	0
Use PMTU	<input checked="" type="checkbox"/> Enabled
TOS	Preserve
Auto-Last Hop	Default
Traffic Group	None

Cancel Repeat Finished

7. Inicie sesión en el clúster de Red Hat OpenShift con privilegios de administrador de clúster.
8. Cree una subred hosten OpenShift para el servidor BIG-IP de F5, que amplía la subred del clúster OpenShift al servidor BIG-IP de F5. Descargue la definición YAML de la subred del host.


```
wget https://github.com/F5Networks/k8s-bigip-ctrl/blob/master/docs/config_examples/openshift/f5-kctr-openshift-hostsubnet.yaml
```

9. Edite el archivo de subred del host y agregue LA IP BIG-IP VTEP (túnel VXLAN) para OpenShift SDN.

```
apiVersion: v1
kind: HostSubnet
metadata:
  name: f5-server
  annotations:
    pod.network.openshift.io/fixed-vnid-host: "0"
    pod.network.openshift.io/assign-subnet: "true"
# provide a name for the node that will serve as BIG-IP's entry into the
cluster
host: f5-server
# The hostIP address will be the BIG-IP interface address routable to
the
# OpenShift Origin nodes.
# This address is the BIG-IP VTEP in the SDN's VXLAN.
hostIP: 10.63.172.239
```



Cambie el hostIP y otros detalles según corresponda a su entorno.

10. Cree el recurso HostSubnet.

```
[admin@rhel-7 ~]$ oc create -f f5-kctr-openshift-hostsubnet.yaml

hostsubnet.network.openshift.io/f5-server created
```

11. Obtenga el intervalo de subred IP del clúster para la subred del host creada para el servidor BIG-IP de F5.

```
[admin@rhel-7 ~]$ oc get hostssubnet
```

NAME	HOST	HOST IP
SUBNET	EGRESS CIDRS	EGRESS IPS
f5-server	f5-server	10.63.172.239
10.131.0.0/23		
ocp-vmw-nszws-master-0	ocp-vmw-nszws-master-0	10.63.172.44
10.128.0.0/23		
ocp-vmw-nszws-master-1	ocp-vmw-nszws-master-1	10.63.172.47
10.130.0.0/23		
ocp-vmw-nszws-master-2	ocp-vmw-nszws-master-2	10.63.172.48
10.129.0.0/23		
ocp-vmw-nszws-worker-r8fh4	ocp-vmw-nszws-worker-r8fh4	10.63.172.7
10.130.2.0/23		
ocp-vmw-nszws-worker-tvr46	ocp-vmw-nszws-worker-tvr46	10.63.172.11
10.129.2.0/23		
ocp-vmw-nszws-worker-wdxhg	ocp-vmw-nszws-worker-wdxhg	10.63.172.24
10.128.2.0/23		
ocp-vmw-nszws-worker-wg8r4	ocp-vmw-nszws-worker-wg8r4	10.63.172.15
10.131.2.0/23		
ocp-vmw-nszws-worker-wtgfw	ocp-vmw-nszws-worker-wtgfw	10.63.172.17
10.128.4.0/23		

12. Cree una autoIP en OpenShift VXLAN con una IP en el rango de subred de host de OpenShift correspondiente al servidor BIG-IP de F5. Inicie sesión en el sistema BIG-IP de F5, desplácese a Red > IP automáticas y haga clic en Crear. Introduzca una dirección IP desde la subred IP del clúster creada para la subred de host BIG-IP de F5, seleccione el túnel VXLAN e introduzca los demás detalles. A continuación, haga clic en finalizado.

The screenshot shows the 'New Self IP...' configuration page in OpenShift. The breadcrumb navigation is 'Network >> Self IPs >> New Self IP...'. The 'Configuration' section contains the following fields:

Name	10.131.0.60
IP Address	10.131.0.60
Netmask	255.252.0.0
VLAN / Tunnel	openshift_vxla
Port Lockdown	Allow All
Traffic Group	<input type="checkbox"/> Inherit traffic group from current partition / path traffic-group-local-only (non-floating)
Service Policy	None

At the bottom of the form, there are three buttons: 'Cancel', 'Repeat', and 'Finished'.

13. Cree una partición en el sistema BIG-IP de F5 que se va a configurar y utilizar con CIS. Vaya a sistema > usuarios > Lista de particiones, haga clic en Crear e introduzca los detalles. A continuación, haga clic en finalizado.

System » Users : Partition List » New Partition...

Properties

Partition Name	<input type="text" value="ocp-vmw"/>
Partition Default Route Domain	<input type="text" value="0"/>
Description	<div style="border: 1px solid #ccc; height: 150px;"></div> <p><input type="checkbox"/> Extend Text Area <input type="checkbox"/> Wrap Text</p>

Redundant Device Configuration

Device Group	<input checked="" type="checkbox"/> Inherit device group from root folder <input type="text" value="None"/>
Traffic Group	<input checked="" type="checkbox"/> Inherit traffic group from root folder <input type="text" value="traffic-group-1 (floating)"/>



F5 recomienda que no se realice ninguna configuración manual en la partición que gestiona CIS.

14. Instale EL F5 BIG-IP CIS utilizando el operador de OperatorHub. Inicie sesión en el clúster de Red Hat OpenShift con privilegios de administración de clúster y cree un secreto con las credenciales de inicio de sesión del sistema BIG-IP de F5, que es un requisito previo para el operador.

```
[admin@rhel-7 ~]$ oc create secret generic bigip-login -n kube-system
--from-literal=username=admin --from-literal=password=admin

secret/bigip-login created
```

15. Instale los CRD de F5 CIS.

```
[admin@rhel-7 ~]$ oc apply -f
https://raw.githubusercontent.com/F5Networks/k8s-bigip-
ctrlr/master/docs/config_examples/crd/Install/customresourcedefinitions.y
ml

customresourcedefinition.apiextensions.k8s.io/virtualservers.cis.f5.com
created
customresourcedefinition.apiextensions.k8s.io/tlsprofiles.cis.f5.com
created
customresourcedefinition.apiextensions.k8s.io/transportservers.cis.f5.co
m created
customresourcedefinition.apiextensions.k8s.io/externaldnss.cis.f5.com
created
customresourcedefinition.apiextensions.k8s.io/ingresslinks.cis.f5.com
created
```

16. Desplácese a Operators > OperatorHub, busque la palabra clave F5 y haga clic en el icono F5 Container Ingresing Service.

OperatorHub

Discover Operators from the Kubernetes community and Red Hat partners, curated by Red Hat. You can purchase commercial software through [Red Hat Marketplace](#). You can install Operators on your clusters to provide optional add-ons and shared services to your developers. After installation, the Operator capabilities will appear in the [Developer Catalog](#) providing a self-service experience.

The screenshot shows the OperatorHub interface. On the left is a navigation menu with categories like AI/Machine Learning, Application Runtime, Big Data, Cloud Provider, Database, Developer Tools, Development Tools, Drivers And Plugins, Integration & Delivery, Logging & Tracing, Modernization & Migration, and Monitoring. The main area is titled 'All Items' and has a search bar containing 'F5'. To the right of the search bar, it says '1 items'. Below the search bar, a single operator card is displayed. The card features the F5 logo, the title 'F5 Container Ingress Services provided by F5 Networks Inc.', and the description 'Operator to install F5 Container Ingress Services (CIS) for BIG-IP.'

17. Lea la información del operador y haga clic en instalar.

F5 Container Ingress Services 1.8.0 provided by F5 Networks Inc.

Install

Latest version
1.8.0

Capability level

- Basic Install
- Seamless Upgrades
- Full Lifecycle
- Deep Insights
- Auto Pilot

Provider type
Certified

Provider
F5 Networks Inc.

Repository
<https://github.com/F5Networks/k8s-bigip-ctlr>

Container image
registry.connect.redhat.com/f5networks/k8s-bigip-ctlr

Introduction

This Operator installs F5 Container Ingress Services (CIS) for BIG-IP in your Cluster. This enables to configure and deploy CIS using Helm Charts.

F5 Container Ingress Services for BIG-IP

F5 Container Ingress Services (CIS) integrates with container orchestration environments to dynamically create L4/L7 services on F5 BIG-IP systems, and load balance network traffic across the services. Monitoring the orchestration API server, CIS is able to modify the BIG-IP system configuration based on changes made to containerized applications.

Documentation

Refer to F5 documentation

- CIS on OpenShift (<https://clouddocs.f5.com/containers/latest/userguide/openshift/>) - OpenShift Routes (<https://clouddocs.f5.com/containers/latest/userguide/routes.html>)

Prerequisites

Create BIG-IP login credentials for use with Operator Helm charts. A basic way be,

```
oc create secret generic <SECRET-NAME> -n kube-system --from-literal=username=<USERNAME> --from-literal=password=<PASSWORD>
```

18. En la pantalla instalar operador, deje todos los parámetros predeterminados y haga clic en instalar.

Install Operator

Install your Operator by subscribing to one of the update channels to keep the Operator up to date. The strategy determines either manual or automatic updates.

Update channel *

beta


Installation mode *

- All namespaces on the cluster (default)
Operator will be available in all Namespaces.
- A specific namespace on the cluster
Operator will be available in a single Namespace only.

Installed Namespace *

Approval strategy *

- Automatic
- Manual

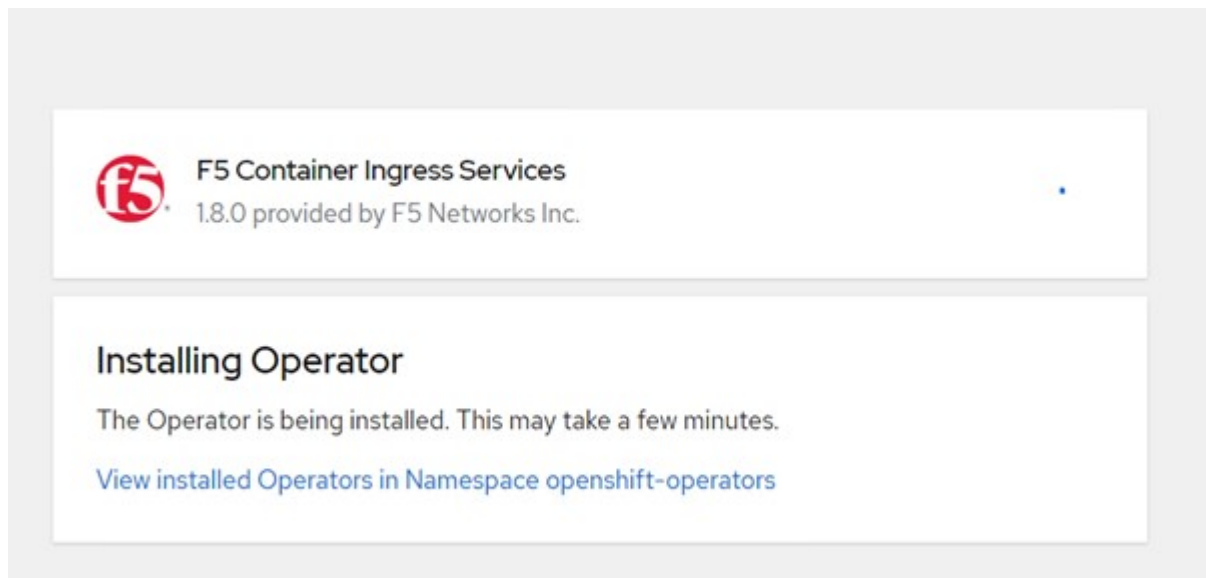
 **F5 Container Ingress Services**
provided by F5 Networks Inc.

Provided APIs

 **F5BigIpCtrlr**

This CRD provides kind `F5BigIpCtrlr` to configure and deploy F5 BIG-IP Controller.

19. Se tarda un rato en instalar el operador.



20. Después de instalar el operador, se muestra el mensaje instalación correcta.

21. Vaya a operadores > operadores instalados, haga clic en F5 Container Ingress Service y, a continuación, haga clic en Crear instancia en el icono F5BigIpctrlr.

[Installed Operators](#) > Operator details



[Details](#) [YAML](#) [Subscription](#) [Events](#) [F5BigIpCtrl](#)

Provided APIs

FBIC F5BigIpCtrl

This CRD provides kind `F5BigIpCtrl` to configure and deploy F5 BIG-IP Controller.

[+ Create instance](#)

22. Haga clic en YAML View y pegue el siguiente contenido después de actualizar los parámetros necesarios.



Actualice los parámetros `bigip_partition`, `"openshift_sdn_name"`, `bigip_url` y.. `bigip_login_secret` a continuación se muestran los valores de la configuración antes de copiar el contenido.

```

apiVersion: cis.f5.com/v1
kind: F5BigIpCtrlr
metadata:
  name: f5-server
  namespace: openshift-operators
spec:
  args:
    log_as3_response: true
    agent: as3
    log_level: DEBUG
    bigip_partition: ocp-vmw
    openshift_sdn_name: /Common/openshift_vxlan
    bigip_url: 10.61.181.19
    insecure: true
    pool-member-type: cluster
    custom_resource_mode: true
    as3_validation: true
    ipam: true
    manage_configmaps: true
  bigip_login_secret: bigip-login
  image:
    pullPolicy: Always
    repo: f5networks/cntr-ingress-svcs
    user: registry.connect.redhat.com
  namespace: kube-system
  rbac:
    create: true
  resources: {}
  serviceAccount:
    create: true
  version: latest

```

23. Después de pegar este contenido, haga clic en Crear. De esta forma se instalan los POD CIS en el espacio de nombres del sistema kube.

Pods Create Pod

Filter Name Search by name... 🔍

Name ↑	Status ↓	Ready ↓	Restarts ↓	Owner ↓	Memory ↓	CPU ↓	
P f5-server-f5-bigip-ctrl-5d7578667d-qxdgj	Running	1/1	0	RS f5-server-f5-bigip-ctrl-5d7578667d	611 MiB	0.003 cores	⋮



Red Hat OpenShift, de forma predeterminada, proporciona una forma de exponer los servicios a través de rutas para el equilibrio de carga L7. Un enrutador OpenShift integrado es responsable de la publicidad y el manejo del tráfico de estas rutas. Sin embargo, también puede configurar F5 CIS para que admita las rutas a través de un sistema BIG-IP externo de F5, que puede ejecutarse como un enrutador auxiliar o como un reemplazo del enrutador OpenShift autoalojado. CIS crea un servidor virtual en EL sistema BIG-IP que actúa como enrutador para las rutas OpenShift y BIG-IP maneja el anuncio y el enrutamiento de tráfico. Consulte la documentación aquí para obtener información sobre los parámetros para habilitar esta función. Tenga en cuenta que estos parámetros se definen para el recurso de implementación de OpenShift en la API de Apps/v1. Por lo tanto, si se usan con la API de recurso `cis.f5.com/v1` de `F5BigIpctrl`, reemplace los guiones (-) por guiones bajos (_) para los nombres de los parámetros.

24. Los argumentos que se pasan a la creación de recursos CIS incluyen `ipam: true` y `custom_resource_mode: true`. Estos parámetros son necesarios para habilitar la integración CIS con un controlador IPAM. Compruebe que CIS ha habilitado la integración IPAM creando el recurso IPAM de F5.

```
[admin@rhel-7 ~]$ oc get f5ipam -n kube-system
```

NAMESPACE	NAME	AGE
kube-system	ipam.10.61.181.19.ocp-vmw	43s

25. Cree la cuenta de servicio, la función y el enlace de rol necesarios para el controlador IPAM de F5. Cree un archivo YAML y pegue el siguiente contenido.

```

[admin@rhel-7 ~]$ vi f5-ipam-rbac.yaml

kind: ClusterRole
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: ipam-ctrl-clusterrole
rules:
  - apiGroups: ["fic.f5.com"]
    resources: ["ipams","ipams/status"]
    verbs: ["get", "list", "watch", "update", "patch"]
---
kind: ClusterRoleBinding
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: ipam-ctrl-clusterrole-binding
  namespace: kube-system
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: ipam-ctrl-clusterrole
subjects:
  - apiGroup: ""
    kind: ServiceAccount
    name: ipam-ctrl
    namespace: kube-system
---
apiVersion: v1
kind: ServiceAccount
metadata:
  name: ipam-ctrl
  namespace: kube-system

```

26. Cree los recursos.

```

[admin@rhel-7 ~]$ oc create -f f5-ipam-rbac.yaml

clusterrole.rbac.authorization.k8s.io/ipam-ctrl-clusterrole created
clusterrolebinding.rbac.authorization.k8s.io/ipam-ctrl-clusterrole-
binding created
serviceaccount/ipam-ctrl created

```

27. Cree un archivo YAML y pegue la definición de implementación de F5 IPAM que se proporciona a continuación.



Actualice el parámetro intervalo ip en `spec.template.spec.Containers[0].args` a continuación para reflejar los rangos de direcciones IP y `ipamLabels` correspondientes a su configuración.



`IpamLabels [range1 y. range2` En ejemplo inferior] es necesario anotar los servicios de tipo `LoadBalancer` para el controlador IPAM a fin de detectar y asignar una dirección IP del intervalo definido.

```

[admin@rhel-7 ~]$ vi f5-ipam-deployment.yaml

apiVersion: apps/v1
kind: Deployment
metadata:
  labels:
    name: f5-ipam-controller
  name: f5-ipam-controller
  namespace: kube-system
spec:
  replicas: 1
  selector:
    matchLabels:
      app: f5-ipam-controller
  template:
    metadata:
      creationTimestamp: null
      labels:
        app: f5-ipam-controller
    spec:
      containers:
      - args:
        - --orchestration=openshift
        - --ip-range='{ "range1": "10.63.172.242-10.63.172.249",
"range2": "10.63.170.111-10.63.170.129"}'
        - --log-level=DEBUG
        command:
        - /app/bin/f5-ipam-controller
        image: registry.connect.redhat.com/f5networks/f5-ipam-
controller:latest
        imagePullPolicy: IfNotPresent
        name: f5-ipam-controller
        dnsPolicy: ClusterFirst
        restartPolicy: Always
        schedulerName: default-scheduler
        securityContext: {}
        serviceAccount: ipam-ctrlr
        serviceAccountName: ipam-ctrlr

```

28. Cree la implementación del controlador IPAM de F5.

```

[admin@rhel-7 ~]$ oc create -f f5-ipam-deployment.yaml

deployment/f5-ipam-controller created

```

29. Compruebe que se están ejecutando los POD del controlador IPAM de F5.

```
[admin@rhel-7 ~]$ oc get pods -n kube-system
```

NAME	READY	STATUS	RESTARTS
f5-ipam-controller-5986cff5bd-2bvn6	1/1	Running	0
30s			
f5-server-f5-bigip-ctrlr-5d7578667d-qxdgj	1/1	Running	0
14m			

30. Cree el esquema F5 IPAM.

```
[admin@rhel-7 ~]$ oc create -f  
https://raw.githubusercontent.com/F5Networks/f5-ipam-  
controller/main/docs/_static/schemas/ipam_schema.yaml  
  
customresourcedefinition.apiextensions.k8s.io/ipams.fic.f5.com
```

Verificación

1. Cree un servicio de tipo LoadBalancer

```
[admin@rhel-7 ~]$ vi example_svc.yaml
```

```
apiVersion: v1
kind: Service
metadata:
  annotations:
    cis.f5.com/ipamLabel: range1
  labels:
    app: f5-demo-test
    name: f5-demo-test
    namespace: default
spec:
  ports:
  - name: f5-demo-test
    port: 80
    protocol: TCP
    targetPort: 80
  selector:
    app: f5-demo-test
  sessionAffinity: None
  type: LoadBalancer
```

```
[admin@rhel-7 ~]$ oc create -f example_svc.yaml
```

```
service/f5-demo-test created
```

2. Compruebe si el controlador IPAM le asigna una IP externa.

```
[admin@rhel-7 ~]$ oc get svc
```

NAME	TYPE	CLUSTER-IP	EXTERNAL-IP
f5-demo-test	LoadBalancer	172.30.210.108	10.63.172.242
80:32605/TCP	27s		

3. Cree una implementación y utilice el servicio LoadBalancer que se ha creado.

```
[admin@rhel-7 ~]$ vi example_deployment.yaml
```

```
apiVersion: apps/v1
kind: Deployment
metadata:
  labels:
    app: f5-demo-test
  name: f5-demo-test
spec:
  replicas: 2
  selector:
    matchLabels:
      app: f5-demo-test
  template:
    metadata:
      labels:
        app: f5-demo-test
    spec:
      containers:
      - env:
        - name: service_name
          value: f5-demo-test
        image: nginx
        imagePullPolicy: Always
        name: f5-demo-test
        ports:
        - containerPort: 80
          protocol: TCP
```

```
[admin@rhel-7 ~]$ oc create -f example_deployment.yaml
```

```
deployment/f5-demo-test created
```

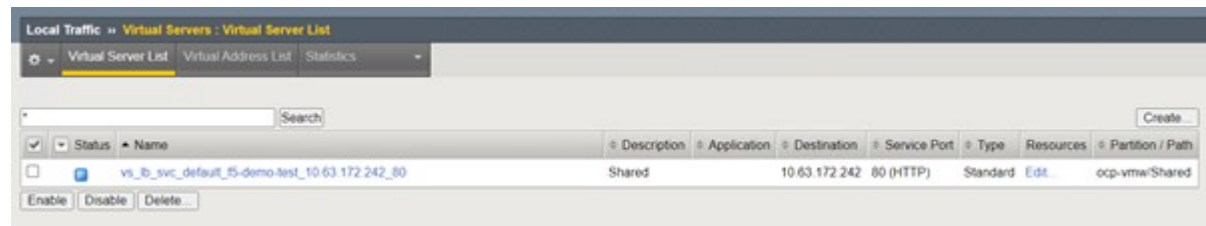
4. Compruebe si los pods están en ejecución.

```
[admin@rhel-7 ~]$ oc get pods
```

NAME	READY	STATUS	RESTARTS	AGE
f5-demo-test-57c46f6f98-47wwp	1/1	Running	0	27s
f5-demo-test-57c46f6f98-cl2m8	1/1	Running	0	27s

5. Compruebe si se crea el servidor virtual correspondiente en EL sistema BIG-IP para el servicio del tipo LoadBalancer en OpenShift. Desplácese a tráfico local > servidores virtuales > Lista de servidores

virtuales.



Creación de registros privados de imágenes

Para la mayoría de implementaciones de Red Hat OpenShift, utilizando un registro público como "Quay.io" o "DockerHub" satisface la mayoría de las necesidades de sus clientes. Sin embargo, hay ocasiones en las que un cliente puede querer alojar sus propias imágenes privadas o personalizadas.

Este procedimiento documenta la creación de un registro de imágenes privadas respaldado por un volumen persistente proporcionado por Trident y NetApp ONTAP.



Astra Control Center requiere un registro para alojar las imágenes que necesitan los contenedores Astra. En la siguiente sección se describen los pasos para configurar un registro privado en el clúster de Red Hat OpenShift e insertar las imágenes necesarias para admitir la instalación de Astra Control Center.

Crear un registro de imágenes privadas

1. Elimine la anotación predeterminada de la clase de almacenamiento predeterminada actual y anote la clase de almacenamiento respaldada por Trident como predeterminada para el clúster OpenShift.

```
[netapp-user@rhel7 ~]$ oc patch storageclass thin -p '{"metadata": {"annotations": {"storageclass.kubernetes.io/is-default-class": "false"}}}'
storageclass.storage.k8s.io/thin patched

[netapp-user@rhel7 ~]$ oc patch storageclass ocp-trident -p '{"metadata": {"annotations": {"storageclass.kubernetes.io/is-default-class": "true"}}}'
storageclass.storage.k8s.io/ocp-trident patched
```

2. Edite el operador imagerRegistry introduciendo los siguientes parámetros de almacenamiento en el spec sección.


```
[netapp-user@rhel7 ~]$ oc edit
configs.imageregistry.operator.openshift.io

storage:
  pvc:
    claim:
```

3. Introduzca los siguientes parámetros en el `spec` Sección para crear una ruta OpenShift con un nombre de host personalizado. Guarde y salga.

```
routes:
- hostname: astra-registry.apps.ocp-vmw.cie.netapp.com
  name: netapp-astra-route
```



La configuración de ruta anterior se utiliza cuando se desea un nombre de host personalizado para la ruta. Si desea que OpenShift cree una ruta con un nombre de host predeterminado, puede agregar los siguientes parámetros al `spec` sección:
`defaultRoute: true.`

Certificados TLS personalizados

Cuando se utiliza un nombre de host personalizado para la ruta, de forma predeterminada, utiliza la configuración TLS predeterminada del operador de OpenShift Ingress. Sin embargo, puede agregar una configuración TLS personalizada a la ruta. Para ello, lleve a cabo los siguientes pasos.

- a. Cree un secreto con los certificados TLS y la clave de la ruta.

```
[netapp-user@rhel7 ~]$ oc create secret tls astra-route-tls -n
openshift-image-registry -cert/home/admin/netapp-astra/tls.crt
--key=/home/admin/netapp-astra/tls.key
```

- b. Edite el operador `imageRegistry` agregue los siguientes parámetros al `spec` sección.

```
[netapp-user@rhel7 ~]$ oc edit
configs.imageregistry.operator.openshift.io

routes:
- hostname: astra-registry.apps.ocp-vmw.cie.netapp.com
  name: netapp-astra-route
  secretName: astra-route-tls
```

4. Vuelva a editar el operador de imageregistry cambie el estado de administración del operador a Managed estado. Guarde y salga.

```
oc edit configs.imageregistry/cluster

managementState: Managed
```

5. Si se cumplen todos los requisitos previos, se crean EVs, POD y servicios para el registro de imágenes privadas. En unos minutos, el registro debería estar activo.

```
[netapp-user@rhel7 ~]$oc get all -n openshift-image-registry
```

NAME	READY	STATUS
pod/cluster-image-registry-operator-74f6d954b6-rb7zr	1/1	Running
3		90d
pod/image-pruner-1627257600-f5cpj	0/1	Completed
0		2d9h
pod/image-pruner-1627344000-swqx9	0/1	Completed
0		33h
pod/image-pruner-1627430400-rv5nt	0/1	Completed
0		9h
pod/image-registry-6758b547f-6pnj8	1/1	Running
0		76m
pod/node-ca-bwb5r	1/1	Running
0		90d
pod/node-ca-f8w54	1/1	Running
0		90d
pod/node-ca-gjx7h	1/1	Running
0		90d
pod/node-ca-lcx4k	1/1	Running
0		33d
pod/node-ca-v7zmx	1/1	Running
0		7d21h
pod/node-ca-xpppp	1/1	Running
0		89d

NAME	TYPE	CLUSTER-IP	EXTERNAL-IP
service/image-registry	ClusterIP	172.30.196.167	<none>
5000/TCP			15h
service/image-registry-operator	ClusterIP	None	<none>
60000/TCP			90d

NAME	DESIRED	CURRENT	READY	UP-TO-DATE
------	---------	---------	-------	------------

```

AVAILABLE      NODE SELECTOR      AGE
daemonset.apps/node-ca      6      6      6      6      6
kubernetes.io/os=linux      90d

NAME                                                    READY  UP-TO-DATE
AVAILABLE      AGE
deployment.apps/cluster-image-registry-operator      1/1    1      1
90d
deployment.apps/image-registry                        1/1    1      1
15h

NAME                                                    DESIRED
CURRENT      READY  AGE
replicaset.apps/cluster-image-registry-operator-74f6d954b6      1      1
1      90d
replicaset.apps/image-registry-6758b547f                1      1
1      76m
replicaset.apps/image-registry-78bfbd7f59              0      0
0      15h
replicaset.apps/image-registry-7fcc8d6cc8              0      0
0      80m
replicaset.apps/image-registry-864f88f5b              0      0
0      15h
replicaset.apps/image-registry-cb47fffb              0      0
0      10h

NAME                                                    COMPLETIONS  DURATION  AGE
job.batch/image-pruner-1627257600                    1/1          10s       2d9h
job.batch/image-pruner-1627344000                    1/1          6s        33h
job.batch/image-pruner-1627430400                    1/1          5s        9h

NAME                                                    SCHEDULE  SUSPEND  ACTIVE  LAST
SCHEDULE  AGE
cronjob.batch/image-pruner      0 0 * * *  False   0      9h
90d

NAME                                                    HOST/PORT
PATH  SERVICES      PORT  TERMINATION  WILDCARD
route.route.openshift.io/public-routes  astra-registry.apps.ocp-
vmw.cie.netapp.com      image-registry  <all>  reencrypt  None

```

6. Si utiliza los certificados TLS predeterminados para la ruta de registro del operador Ingress OpenShift, puede obtener los certificados TLS utilizando el siguiente comando.

```
[netapp-user@rhel7 ~]$ oc extract secret/router-ca --keys=tls.crt -n openshift-ingress-operator
```

7. Para permitir que los nodos de OpenShift accedan a las imágenes y las extractivas del Registro, agregue los certificados al cliente docker en los nodos de OpenShift. Cree un mapa de configuración en `openshift-config` Espacio de nombres mediante los certificados TLS y retome la configuración de la imagen del clúster para garantizar la confianza del certificado.

```
[netapp-user@rhel7 ~]$ oc create configmap astra-ca -n openshift-config --from-file=astra-registry.apps.ocp-vmw.cie.netapp.com=tls.crt

[netapp-user@rhel7 ~]$ oc patch image.config.openshift.io/cluster --patch '{"spec":{"additionalTrustedCA":{"name":"astra-ca"}}}' --type=merge
```

8. El registro interno de OpenShift se controla mediante autenticación. Todos los usuarios de OpenShift pueden tener acceso al registro de OpenShift, pero las operaciones que el usuario que ha iniciado sesión puede realizar dependen de los permisos del usuario.
 - a. Para permitir que un usuario o un grupo de usuarios extraiga imágenes del Registro, el usuario debe tener asignada la función de visor del Registro.

```
[netapp-user@rhel7 ~]$ oc policy add-role-to-user registry-viewer ocp-user

[netapp-user@rhel7 ~]$ oc policy add-role-to-group registry-viewer ocp-user-group
```

- b. Para permitir a un usuario o grupo de usuarios escribir o insertar imágenes, el usuario debe tener asignado el rol de editor de registros.

```
[netapp-user@rhel7 ~]$ oc policy add-role-to-user registry-editor ocp-user

[netapp-user@rhel7 ~]$ oc policy add-role-to-group registry-editor ocp-user-group
```

9. Para que los nodos OpenShift accedan al Registro y push o extran las imágenes, debe configurar un secreto de extracción.

```
[netapp-user@rhel7 ~]$ oc create secret docker-registry astra-registry-credentials --docker-server=astra-registry.apps.ocp-vmw.cie.netapp.com --docker-username=ocp-user --docker-password=password
```

10. Este secreto de extracción se puede aplicar a las cuentas de servicio o hacer referencia a ellas en la definición de POD correspondiente.

a. Para aplicar revisiones a las cuentas de servicio, ejecute el siguiente comando.

```
[netapp-user@rhel7 ~]$ oc secrets link <service_account_name> astra-registry-credentials --for=pull
```

b. Para hacer referencia al secreto de extracción en la definición de POD, agregue el siguiente parámetro al spec sección.

```
imagePullSecrets:  
  - name: astra-registry-credentials
```

11. Para insertar o extraer una imagen de estaciones de trabajo aparte del nodo OpenShift, lleve a cabo los siguientes pasos.

a. Agregue los certificados TLS al cliente docker.

```
[netapp-user@rhel7 ~]$ sudo mkdir /etc/docker/certs.d/astra-registry.apps.ocp-vmw.cie.netapp.com  
  
[netapp-user@rhel7 ~]$ sudo cp /path/to/tls.crt  
/etc/docker/certs.d/astra-registry.apps.ocp-vmw.cie.netapp.com
```

b. Inicie sesión en OpenShift con el comando de inicio de sesión de OC.

```
[netapp-user@rhel7 ~]$ oc login --token=sha256~D49SpB_lesSrJYwrM0LIO-VRcjWHu0a27vKa0 --server=https://api.ocp-vmw.cie.netapp.com:6443
```

c. Inicie sesión en el registro utilizando las credenciales de usuario de OpenShift con el comando podman/docker.

podman

```
[netapp-user@rhel7 ~]$ podman login astra-registry.apps.ocp-vmw.cie.netapp.com -u kubeadmin -p $(oc whoami -t) --tls -verify=false
```

+ NOTA: Si está utilizando kubeadmin usuario para iniciar sesión en el registro privado, utilice token en lugar de contraseña.

docker

```
[netapp-user@rhel7 ~]$ docker login astra-registry.apps.ocp-vmw.cie.netapp.com -u kubeadmin -p $(oc whoami -t)
```

+ NOTA: Si está utilizando kubeadmin usuario para iniciar sesión en el registro privado, utilice token en lugar de contraseña.

d. Empuje o tire de las imágenes.

podman

```
[netapp-user@rhel7 ~]$ podman push astra-registry.apps.ocp-vmw.cie.netapp.com/netapp-astra/vault-controller:latest  
[netapp-user@rhel7 ~]$ podman pull astra-registry.apps.ocp-vmw.cie.netapp.com/netapp-astra/vault-controller:latest
```

docker

```
[netapp-user@rhel7 ~]$ docker push astra-registry.apps.ocp-vmw.cie.netapp.com/netapp-astra/vault-controller:latest  
[netapp-user@rhel7 ~]$ docker pull astra-registry.apps.ocp-vmw.cie.netapp.com/netapp-astra/vault-controller:latest
```

Información de copyright

Copyright © 2024 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.