Table of Contents

Exploring load balancer options: Red Hat OpenShift with NetApp ................................................. 1
Installing MetalLB load balancers: Red Hat OpenShift with NetApp .............................................. 1
Installing F5 BIG-IP Load Balancers .......................................................................................... 3
Exploring load balancer options: Red Hat OpenShift with NetApp

In most cases, Red Hat OpenShift makes applications available to the outside world through routes. A service is exposed by giving it an externally reachable hostname. The defined route and the endpoints identified by its service can be consumed by an OpenShift router to provide this named connectivity to external clients.

However in some cases, applications require the deployment and configuration of customized load balancers to expose the appropriate services. One example of this is NetApp Astra Control Center. To meet this need, we have evaluated a number of custom load balancer options. Their installation and configuration are described in this section.

The following pages have additional information about load balancer options validated in the Red Hat OpenShift with NetApp solution:

- MetalLB
- F5 BIG-IP

Installing MetalLB load balancers: Red Hat OpenShift with NetApp

This page lists the installation and configuration instructions for the MetalLB load balancer.

MetalLB is a self-hosted network load balancer installed on your OpenShift cluster that allows the creation of OpenShift services of type load balancer in clusters that do not run on a cloud provider. The two main features of MetalLB that work together to support LoadBalancer services are address allocation and external announcement.

MetalLB configuration options

Based on how MetalLB announces the IP address assigned to LoadBalancer services outside of the OpenShift cluster, it operates in two modes:

- **Layer 2 mode.** In this mode, one node in the OpenShift cluster takes ownership of the service and responds to ARP requests for that IP to make it reachable outside of the OpenShift cluster. Because only the node advertises the IP, it has a bandwidth bottleneck and slow failover limitations. For more information, see the documentation [here](#).

- **BGP mode.** In this mode, all nodes in the OpenShift cluster establish BGP peering sessions with a router and advertise the routes to forward traffic to the service IPs. The prerequisite for this is to integrate MetalLB with a router in that network. Owing to the hashing mechanism in BGP, it has certain limitation when IP-to-Node mapping for a service changes. For more information, refer to the documentation [here](#).

For the purpose of this document, we are configuring MetalLB in layer-2 mode.

Installing The MetalLB Load Balancer

1. Download the MetalLB resources.
2. Edit file `metallb.yaml` and remove `spec.template.spec.securityContext` from controller Deployment and the speaker DaemonSet.

**Lines to be deleted:**

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

3. Create the `metallb-system` namespace.

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

4. Create the MetalLB CR.

```bash
[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. Before configuring the MetalLB speaker, grant the speaker DaemonSet elevated privileges so that it can perform the networking configuration required to make the load balancers work.

```
[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 by creating a ConfigMap in the metallb-system namespace.

```
[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. Now when loadbalancer services are created, MetalLB assigns an externalIP to the services and advertises the IP address by responding to ARP requests.

If you wish to configure MetalLB in BGP mode, skip step 6 above and follow the procedure in the MetalLB documentation here.

## Installing F5 BIG-IP Load Balancers

F5 BIG-IP is an Application Delivery Controller (ADC) that offers a broad set of advanced production-grade traffic management and security services like L4-L7 load balancing, SSL/TLS offload, DNS, firewall and many more. These services drastically increase the availability, security and performance of your applications.

F5 BIG-IP can be deployed and consumed in various ways, on dedicated hardware, in the cloud, or as a virtual appliance on-premises. Refer to the documentation here to explore and deploy F5 BIG-IP as per requirement.

For efficient integration of F5 BIG-IP services with Red Hat OpenShift, F5 offers the BIG-IP Container Ingress Service (CIS). CIS is installed as a controller pod that watches OpenShift API for certain Custom Resource Definitions (CRDs) and manages the F5 BIG-IP system configuration. F5 BIG-IP CIS can be configured to
control service types LoadBalancers and Routes in OpenShift.

Further, for automatic IP address allocation to service the type LoadBalancer, you can utilize the F5 IPAM controller. The F5 IPAM controller is installed as a controller pod that watches OpenShift API for LoadBalancer services with an ipamLabel annotation to allocate the IP address from a preconfigured pool.

This page lists the installation and configuration instructions for F5 BIG-IP CIS and IPAM controller. As a prerequisite, you must have an F5 BIG-IP system deployed and licensed. It must also be licensed for SDN services, which are included by default with the BIG-IP VE base license.

F5 BIG-IP can be deployed in standalone or cluster mode. For the purpose of this validation, F5 BIG-IP was deployed in standalone mode, but, for production purposes, it is preferred to have a cluster of BIG-IPS to avoid a single point of failure.

An F5 BIG-IP system can be deployed on dedicated hardware, in the cloud, or as a virtual appliance on-premises with versions greater than 12.x for it to be integrated with F5 CIS. For the purpose of this document, the F5 BIG-IP system was validated as a virtual appliance, for example using the BIG-IP VE edition.

**Validated releases**

<table>
<thead>
<tr>
<th>Technology</th>
<th>Software version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red Hat OpenShift</td>
<td>4.6 EUS, 4.7</td>
</tr>
<tr>
<td>F5 BIG-IP VE edition</td>
<td>16.1.0</td>
</tr>
<tr>
<td>F5 Container Ingress Service</td>
<td>2.5.1</td>
</tr>
<tr>
<td>F5 IPAM Controller</td>
<td>0.1.4</td>
</tr>
<tr>
<td>F5 AS3</td>
<td>3.30.0</td>
</tr>
</tbody>
</table>

**Installation**

1. Install the F5 Application Services 3 extension to allow BIG-IP systems to accept configurations in JSON instead of imperative commands. Go to [F5 AS3 GitHub repository](#), and download the latest RPM file.
2. Log into F5 BIG-IP system, navigate to iApps > Package Management LX and click Import.
3. Click Choose File and select the downloaded AS3 RPM file, click OK, and then click Upload.
4. Confirm that the AS3 extension is installed successfully.
5. Next configure the resources required for communication between OpenShift and BIG-IP systems. First create a tunnel between OpenShift and the BIG-IP server by creating a VXLAN tunnel interface on the BIG-IP system for OpenShift SDN. Navigate to Network > Tunnels > Profiles, click Create, and set the Parent Profile to vxlan and the Flooding Type to Multicast. Enter a name for the profile and click Finished.

6. Navigate to Network > Tunnels > Tunnel List, click Create, and enter the name and local IP address for the tunnel. Select the tunnel profile that was created in the previous step and click Finished.

7. Log into the Red Hat OpenShift cluster with cluster-admin privileges.
8. Create a hostsubnet on OpenShift for the F5 BIG-IP server, which extends the subnet from the OpenShift cluster to the F5 BIG-IP server. Download the host subnet YAML definition.

   *wget https://github.com/F5Networks/k8s-bigip-ctlr/blob/master/docs/config_examples/openshift/f5-kctlr-openshift-hostsubnet.yaml*

9. Edit the host subnet file and add the BIG-IP VTEP (VXLAN tunnel) IP for the OpenShift SDN.

   ```yaml
   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
   ```

   *Change the hostIP and other details as applicable to your environment.*

10. Create the HostSubnet resource.

    ```bash
    [admin@rhel-7 ~]$ oc create -f f5-kctlr-openshift-hostsubnet.yaml
    hostsubnet.network.openshift.io/f5-server created
    ```

11. Get the cluster IP subnet range for the host subnet created for the F5 BIG-IP server.
12. Create a self IP on OpenShift VXLAN with an IP in OpenShift's host subnet range corresponding to the F5 BIG-IP server. Log into the F5 BIG-IP system, navigate to Network > Self IPs and click Create. Enter an IP from the cluster IP subnet created for F5 BIG-IP host subnet, select the VXLAN tunnel, and enter the other details. Then click Finished.
13. Create a partition in the F5 BIG-IP system to be configured and used with CIS. Navigate to System > Users > Partition List, click Create, and enter the details. Then click Finished.

![Partition Configuration](image)

- **Properties**
  - **Partition Name**: ocp-vmw
  - **Partition Default Route Domain**: 0

- **Redundant Device Configuration**
  - **Device Group**: Inherit device group from root folder
  - **Traffic Group**: Inherit traffic group from root folder

**i** F5 recommends that no manual configuration be done on the partition that is managed by CIS.

14. Install the F5 BIG-IP CIS using the operator from OperatorHub. Log into the Red Hat OpenShift cluster with cluster-admin privileges and create a secret with F5 BIG-IP system login credentials, which is a prerequisite for the operator.
15. Install the F5 CIS CRDs.

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

```
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.com created
customresourcedefinition.apiextensions.k8s.io/externaldnss.cis.f5.com created
customresourcedefinition.apiextensions.k8s.io/ingresslinks.cis.f5.com created
```

16. Navigate to Operators > OperatorHub, search for the keyword F5, and click the F5 Container Ingress Service tile.

**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.
17. Read the operator information and click Install.

18. On the Install operator screen, leave all default parameters, and click Install.
19. It takes a while to install the operator.

20. After the operator is installed, the Installation Successful message is displayed.

21. Navigate to Operators > Installed Operators, click F5 Container Ingress Service, and then click Create Instance under the F5BigIpCtr tile.
22. Click YAML View and paste the following content after updating the necessary parameters.

Update the parameters `bigip_partition`, `openshift_sdn_name`, `bigip_url` and `bigip_login_secret` below to reflect the values for your setup before copying the content.
apiVersion: cis.f5.com/v1
kind: F5BigIpCtlr
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. After pasting this content, click Create. This installs the CIS pods in the kube-system namespace.
Red Hat OpenShift, by default, provides a way to expose the services via Routes for L7 load balancing. An inbuilt OpenShift router is responsible for advertising and handling traffic for these routes. However, you can also configure the F5 CIS to support the Routes through an external F5 BIG-IP system, which can run either as an auxiliary router or a replacement to the self-hosted OpenShift router. CIS creates a virtual server in the BIG-IP system that acts as a router for the OpenShift routes, and BIG-IP handles the advertisement and traffic routing. Refer to the documentation here for information on parameters to enable this feature. Note that these parameters are defined for OpenShift Deployment resource in the apps/v1 API. Therefore, when using these with the F5BigIpCtir resource cis.f5.com/v1 API, replace the hyphens (-) with underscores (_) for the parameter names.

24. The arguments that are passed to the creation of CIS resources include `ipam: true` and `custom_resource_mode: true`. These parameters are required for enabling CIS integration with an IPAM controller. Verify that the CIS has enabled IPAM integration by creating the F5 IPAM resource.

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

<table>
<thead>
<tr>
<th>NAMESPACE</th>
<th>NAME</th>
<th>AGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>kube-system</td>
<td>ipam.10.61.181.19.ocp-vmw</td>
<td>43s</td>
</tr>
</tbody>
</table>

25. Create the service account, role and rolebinding required for the F5 IPAM controller. Create a YAML file and paste the following content.
Create the resources.

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

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

Create a YAML file and paste the F5 IPAM deployment definition provided below.
Update the ip-range parameter in spec.template.spec.containers[0].args below to reflect the
ipamLabels and IP address ranges corresponding to your setup.

ipamLabels [range1 and range2 in below example] are required to be annotated for the
services of type LoadBalancer for the IPAM controller to detect and assign an IP address
from the defined range.

```
[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-ctlr
serviceAccountName: ipam-ctlr
```
28. Create the F5 IPAM controller deployment.

```bash
$ oc create -f f5-ipam-deployment.yaml
deployment/f5-ipam-controller created
```

29. Verify the F5 IPAM controller pods are running.

```bash
$ oc get pods -n kube-system
```

<table>
<thead>
<tr>
<th>NAME</th>
<th>READY</th>
<th>STATUS</th>
<th>RESTARTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>f5-ipam-controller-5986cff5bd-2bvn6</td>
<td>1/1</td>
<td>Running</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>30s</td>
<td></td>
</tr>
<tr>
<td>f5-server-f5-bigip-ctlr-5d7578667d-qxdgj</td>
<td>1/1</td>
<td>Running</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>14m</td>
<td></td>
</tr>
</tbody>
</table>

30. Create the F5 IPAM schema.

```bash
$ oc create -f https://raw.githubusercontent.com/F5Networks/f5-ipam-controller/main/docs/_static/schemas/ipam_schema.yaml
```

```yaml
customresourcedefinition.apiextensions.k8s.io/ipams.fic.f5.com
```

**Verification**

1. Create a service of type 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. Check if the IPAM controller assigns an external IP to it.

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

```
NAME           TYPE           CLUSTER-IP       EXTERNAL-IP
PORT(S)        AGE            
---            ----            ---------        ------------
```

```
```

3. Create a deployment and use the LoadBalancer service that was created.
[admin@rhel-7 ~]$ vi example_deployment.yaml

```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. Check if the pods are running.

[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. Check if the corresponding virtual server is created in the BIG-IP system for the service of type LoadBalancer in OpenShift. Navigate to Local Traffic > Virtual Servers > Virtual Server List.
<table>
<thead>
<tr>
<th>Status</th>
<th>Name</th>
<th>Description</th>
<th>Application</th>
<th>Destination</th>
<th>Service Port</th>
<th>Type</th>
<th>Resources</th>
<th>Partition</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>vs_rsvc_default_f5-demo-test_10.63.172.242_80</td>
<td>Shared</td>
<td>10.63.172.242</td>
<td>80 (HTTP)</td>
<td>Standard</td>
<td>Edit</td>
<td>ocp-vmo/Shared</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>