Deploy BIG-IP VE in Oracle Cloud Infrastructure (OCI)

Complete the tasks in this guide to configure two highly-available, multi-NIC BIG-IP VE instances in Oracle Cloud.

BIG-IP VE 13.1.0.4 and later are supported.

This guide uses the following example IP addresses.

BIG-IP A

	Subnet	VNIC/Interface	Private IP	Secondary Private IP
Management	10.0.0.0/24	1.0	10.0.0.2	
External	10.0.1.0/24	1.1	10.0.1.2	10.0.1.202
Internal	10.0.2.0/24	1.2	10.0.2.2	
HA	10.0.2.0/24	1.3	10.0.3.2	

BIG-IP B

	Subnet	VNIC/Interface	Private IP	Secondary Private IP
Management	10.0.0.0/24	1.0	10.0.0.3	
External	10.0.1.0/24	1.1	10.0.1.3	
Internal	10.0.2.0/24	1.2	10.0.2.3	
HA	10.0.2.0/24	1.3	10.0.3.3	

When BIG-IP A fails over to BIG-IP B, the secondary private IP address on BIG-IP A is reassigned to BIG-IP B. This secondary IP address is the virtual IP address for application traffic.

Configure your network

You must first create the network where you will deploy BIG-IP VE. If you have an existing network, you may not need these tasks. However, ensure you update your security lists to allow traffic to BIG-IP VE for management and high availability access.

Create a compartment in OCI

If you don't have an existing compartment, you must first create a compartment to contain your resources.

1. Open the OCI console, log in/register, select your tenancy, click the Home menu, and then under the **Identity** section, click **Compartments**.
2. Click **Create Compartment**.
3. Type a name and description and click **Create Compartment**.

Create a Virtual Cloud Network (VCN)

If you don't have an existing network, create one.

1. In the OCI console, under the **Networking** section, click **Virtual Cloud Networks**.
2. Click **Create Virtual Cloud Network**, and then complete the following fields:

Name	Enter a name.
Create virtual cloud network only	Click to enable this option.
CIDR Block	10.0.0.0/16

3. Leave all other settings with the default values, and then click **Create Virtual Cloud Network**.

Create four subnets

This deployment has four subnets:

- **External, public subnet**—where you'll create a virtual server to accept Internet traffic.
- **Internal, private subnet**—where your application servers live.
- **Management subnet**—where you can access the BIG-IP Configuration utility; you use the Configuration utility to configure BIG-IP VE.
- **High availability subnet**—to sync configuration.

Now create these four subnets.

1. Under the **Networking** section, click **Virtual Cloud Networks**.
2. Click the name of your **VCN**.
3. From the left menu, click **Subnets**.

4. Click **Create Subnet** and create the following subnets.

   Expand the **Availability Domain** list and ensure all four subnets are within the same domain (for example, set all to **PHX-AD-1**).

Subnet Name	CIDR Block	Route Table	Public or Private
Management	10.0.0.0/24	Default	Public Subnet
External	10.0.1.0/24	Default	Public Subnet
Internal	10.0.2.0/24	Default	Public Subnet
HA	10.0.3.0/24	Default	Private Subnet

5. Leave other defaults and then click **Create**.

Update Security List

You must allow traffic into the ports required for BIG-IP VE management, for your application, and for high availability.

1. Under the **Networking** section, click **Virtual Cloud Networks**.
2. Click the name of your VCN.
3. From the left menu, click **Security Lists**, and then click the name of the default security list for your VCN.
4. Click **Edit All Rules**.
5. Change the Allow Rules for Ingress to ensure you have these rules:

Source Type	Source CIDR	IP Protocol	Source Port Range	Destination Port Range
CIDR	A range of IP addresses on your network	TCP	All	22
CIDR	A range of IP addresses on your network	ICMP	All	All
CIDR	A range of IP addresses on your network	TCP	All	443 for BIG-IP VE management access
CIDR	A range of IP addresses on your network	TCP	All	4353
CIDR	A range of IP addresses on your network	TCP	All	6699
CIDR	A range of IP addresses on your network	**UDP**	All	1026

6. When done, click **Save Security List Rules**.

Create an Internet gateway

By default, traffic from the management and external subnets cannot leave the VPC. You must add an Internet gateway.

1. Under the **Networking** section, click **Virtual Cloud Networks**.

2. Click the name of your VCN.
3. From the left menu, click **Internet Gateways**.
4. Ensure you choose the same compartment you've used in all previous procedures.
5. Enter a **Name**, and then click **Create Internet Gateway**.

Create a route rule for the Internet gateway

You must associate the gateway with your route table.

1. Under the **Networking** section, click **Virtual Cloud Networks**.
2. Click the name of your VCN.
3. From the left menu, click **Route Tables**.
4. Click the name of the default route table for your VCN.
5. Click **Edit Route Rules**, and then click **+ Another Route Rule**.
6. Complete the following information:

Target Type	Destination CIDR Block	Compartment	Target Internet Gateway
Internet Gateway	0.0.0.0/0	Leave as your compartment	Gateway you created in previous task

7. Click **Save**.

Deploy BIG-IP VE A

You will create two instances of BIG-IP VE. This guide refers to the first instance as **BIG-IP A**.

Download a BIG-IP VE image

Now you must download a BIG-IP VE image (a .qcow2.zip file). You will upload this image to Oracle storage.

1. Open a browser, visit the F5 Downloads page, and then log in or register.
2. On the **Downloads Overview** page, click **Find a Download**.
3. Under **Product Line**, click **BIG-IP <version>/Virtual Edition**, where <version> is the version you want to download.
4. Under **Name**, click **x.x.x.x_Virtual-Edition**, where x.x.x.x is the product container you want to download, and then at the license agreement notification click **I Accept**.
   Notes:
   BIG-IP VE 13.1.0.4 and later are supported.
   1SLOT images do not leave room for upgrade.
5. Under **Filename**, click one of the **.qcow2.zip** image files.
6. Choose the download location closest to you.

7. When the file finishes downloading, unzip the **.qcow2.zip** file to a local drive.
   Tip: For Windows, use *7-Zip* or for Linux or Mac, use *unzip*.
8. Once unzipped, if necessary extract the **.qcow2** from the .tar file with **tar xvfz <filename>.tar**, using *7-Zip*.

Create a storage bucket and pre-authenticated request

Create an OCI object storage bucket, and then upload the .qcow2 file.

1. In the OCI console, under the **Storage** section, click **Object Storage**.
2. In the **Compartment** list, select your compartment, and then click **Create Bucket**.
3. In the BUCKET NAME box, enter a name, leave all settings with default values, and then click **Create Bucket**.
4. In the center pane, find your bucket, hover your mouse over the **...**, and then on the pop-up menu select **Create Pre-Authenticated Request**.
5. In the **NAME** box, enter a name, in the EXPIRATION DATE/TIME box, select a date for expiration, leave all other settings with the default values, and then click **Create Pre-Authenticated Request** and **Close**.
6. Click your storage bucket name, under **Objects**, click **Upload Object**, browse for the **.qcow2** file you downloaded in the previous procedure, and then click **Upload Object**.
7. The OCI Console provides the PRE-AUTHENTICATED REQUEST URL. Next to your object, click **…**, select **Details**, and then copy the **URL Path** for use in the next procedure.

Create a custom image

Now create a custom image. You will use this image as the source of your BIG-IP VE instances.

1. Under the **Compute** section, click **Custom Images**.
2. Click **Import Image**.
3. In the **Name** box, enter a name, expand the **Operating System** list, select **Linux**.
4. In the **Object Storage Url** box, paste the URL for the Pre-Authenticated Request you copied in step 7 of the previous procedure.
5. Under **Image Type** click the **qcow2** option.
6. Under **Launch Mode** click the **Emulated Mode** option.
7. Click **Import Image**.

The import process starts and can take several minutes. When the import is complete, the tile next to the image name changes from orange to green.

Deploy a BIG-IP VE instance

Deploy a BIG-IP VE instance from the custom image you created in the previous procedure. This instance is referred to as **BIG-IP A**.

1. Under the **Compute** section, click **Instances**.
2. Click **Create Instance**.
3. In the **NAME** box, enter a name, and then expand the **Availability Domain** list and select the same availability domain you selected when creating your VCN subnets.
4. Under **Boot Volume** click the **Custom Image** option, expand the **Image** textbox, and select the image you created in the previous procedure.
5. Under the BOOT VOLUME SIZE (IN GB) section is the size of the volume for the image you uploaded. This value will change from version to version. To create a larger initial boot volume, click the **Custom Boot Volume Size** checkbox and enter the volume size.
6. Under SHAPE TYPE, click **Virtual Machine**.
7. Expand the SHAPE list and select an appropriate shape based on your requirements. Shapes restrict the number of vCPUs, VNICs, and allocated memory.

   BIG-IP VE Requirements: https://support.f5.com/csp/article/K14810

   Overview of the instance shapes within OCI: https://docs.us-phoenix-1.oraclecloud.com/Content/Compute/Concepts/computeoverview.htm
8. Under Networking, expand the **Subnet** list and select the management subnet.
9. If you want to access BIG-IP directly from the internet, click the **Assign Public IP Address** checkbox.
10. Click **Create Instance**.

When the instance is ready, the tile next to the instance name changes from orange to green.

Create three VNICs and reboot

When you created the instance, a primary VNIC was created automatically. This VNIC is for management traffic.

You must create three more VNICs for the other subnet traffic.

Important: Ensure the BIG-IP VE instance is running.

1. Under the **Compute** section, click **Instances**.
2. Click the name of your instance.
3. In the left menu, click **Attached VNICs**.
4. Click **Create VNIC** and complete the information for each VNIC:

Name	Virtual Cloud Network	Subnet	Private IP address	Assign public IP address
External	Your VCN	External	10.0.1.2	Enable
Internal	Your VCN	Internal	10.0.2.2	Disable

HA	Your VCN	HA	10.0.3.2	Disable

5. Click **Create VNIC** for each VNIC.
6. Now reboot BIG-IP VE. Click your instance, click **Reboot**, leave the default selection, and then click **OK**.

Important: You must reboot for BIG-IP VE to recognize the VNICs.

License BIG-IP VE

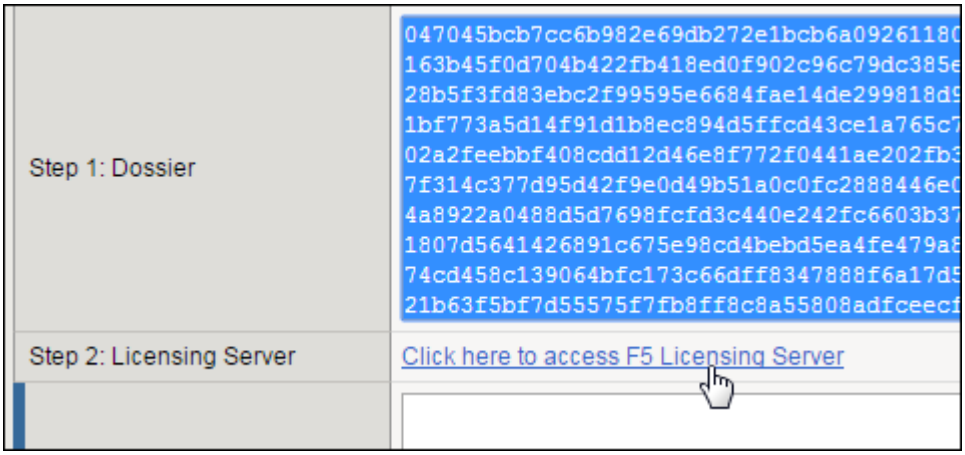
You must enter license information before you can use BIG-IP VE.

1. Open a web browser and log in to the BIG-IP Configuration utility by using https with your Primary VNIC's public IP Address, for example: https://<external-ip-address>. The username is **root** and password is **default**.
2. On the Setup Utility Welcome page, click **Next**.
3. On the General Properties page, click **Activate**.
4. In the Base Registration key field, enter the case-sensitive registration key from F5.

   For **Activation Method**, if you have a production or Eval license, choose **Automatic** and click **Next**.

   If you chose **Manual,** do the following:

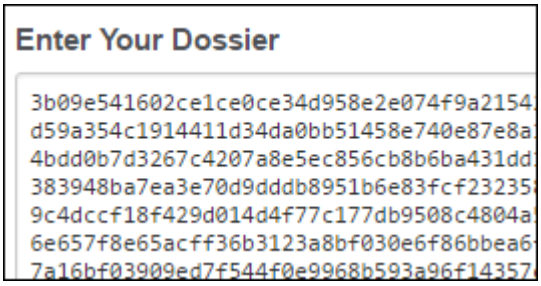
   a. In the **Step 1: Dossier** field, copy all of the text and then **Click here to access F5 Licensing Server**.

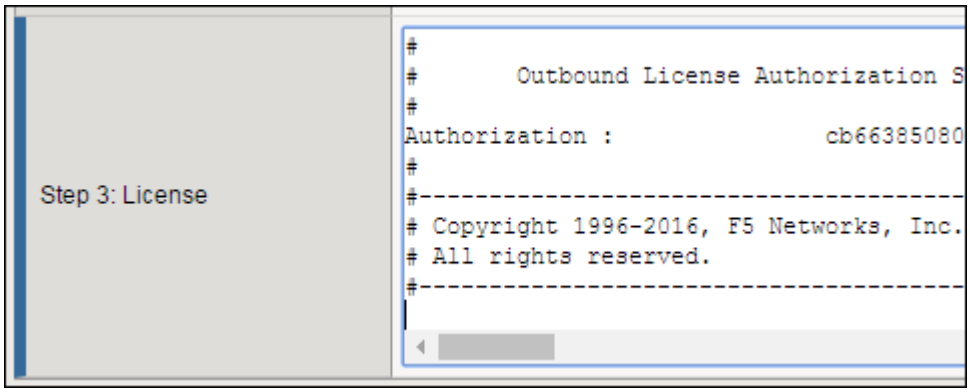
   A separate web page opens.

   b. On the new page, click **Activate License**.

   c. In the **Enter your dossier** field, paste the text and click **Next**.



5. Accept the agreement and click **Continue**.
6. On the Activate F5 Product page, copy the license text in the box. Now go back to the BIG-IP Configuration utility and paste the text into the **Step 3: License** field.

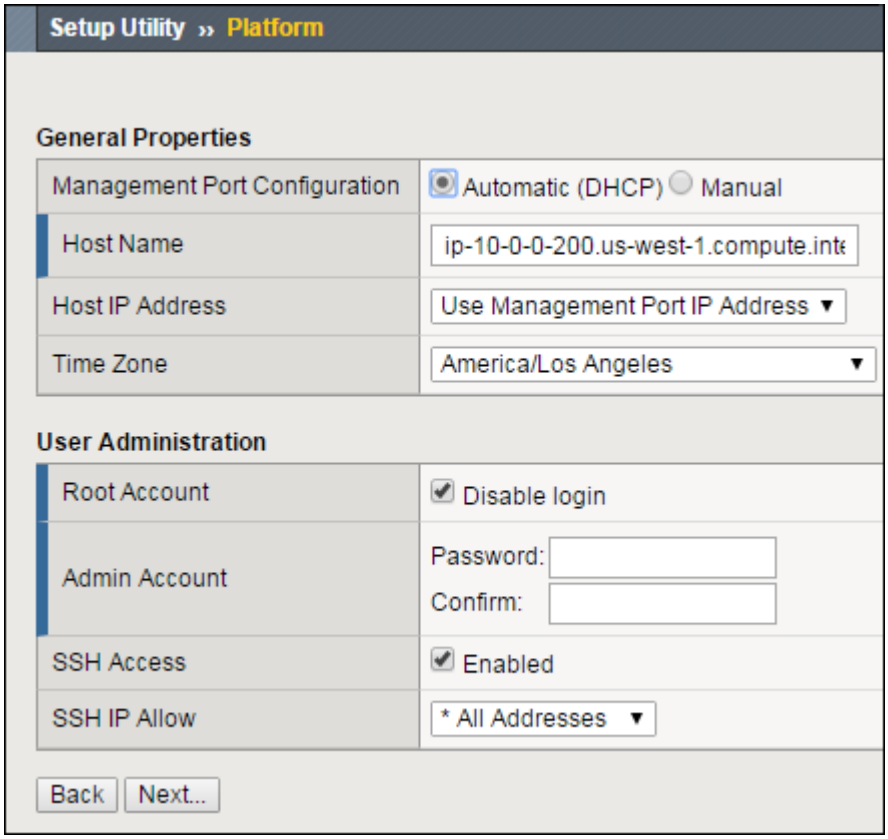


7. Click **Next**.
8. The BIG-IP VE system registers the license and logs you out. When the configuration change is successful, click **Continue** to provision BIG-IP VE.

Provision BIG-IP VE

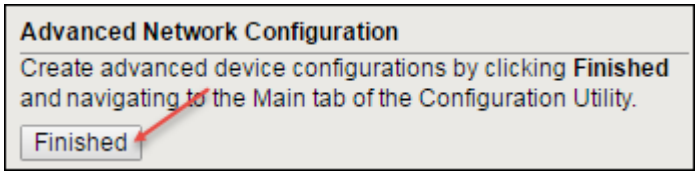
You must confirm the modules you want to run before you can begin to work in the BIG-IP Configuration utility.

1. Open a web browser and log in to the BIG-IP Configuration utility.
2. On the **Resource Provisioning** screen, change settings if necessary and click **Next**.
3. On the **Device Certificates** screen, click **Next.**
4. On the **Platform** screen, in the **Admin Account** field, re-enter the password for the admin account and click **Next**.



BIG-IP VE logs you out.

5. When you log back in, on the **Setup Utility -> Network** screen, in the **Advanced Network Configuration** area, click **Finished**.



Create three VLANs¶

In BIG-IP VE, you must create an external and internal VLAN that corresponds to the Oracle subnets.

1. In the BIG-IP VE Configuration utility, on the Setup Utility Network page, under Advanced Network Configuration, click **Finished**.
2. On the Main tab, click **Network** -> **VLANs**.
3. Click **Create** and populate the appropriate fields for the external VLAN.

Field	Value
Name	External
Interface	1.1
Tagging	Untagged

4. Click **Finished**.

5. Now click **Create** again and populate the appropriate fields for the internal VLAN.

Field	Value
Name	Internal
Interface	1.2
Tagging	Untagged

6. Click **Finished**.
7. Click **Create** and fill in the appropriate fields for the HA VLAN.

Field	Value
Name	HA
Interface	1.3
Tagging	Untagged

8. Click **Finished**.

Create three self IPs¶

Before starting these steps, in OCI, note the primary private IP addresses for the external, internal, and HA network interface.

Then in BIG-IP VE, create an external and internal self IP address, based on these private IP addresses. In the BIG-IP VE Configuration utility, on the Main tab, click **Network -> Self IPs**.

1. Click **Create** and populate the appropriate fields for the external self IP address.

Field	Value
Name	ExternalSelfIP
IP Address	10.0.1.2
Netmask	255.255.255.0
VLAN/Tunnel	external
Port Lockdown	Allow All

2. Click **Repeat** and populate the appropriate fields for the internal self IP address.

Field	Value
Name	InternalSelfIP
IP Address	10.0.2.2
Netmask	255.255.255.0
VLAN/Tunnel	internal
Port Lockdown	Allow All

3. Click **Repeat** and populate the appropriate fields for the HA self IP address.

Field	Value
Name	HASelfIP
IP Address	10.0.3.2
Netmask	255.255.255.0
VLAN/Tunnel	HA
Port Lockdown	Allow All

4. Click **Finished**.

The screen refreshes, and the three new self IP addresses are in the list.

Create a pool and add members to it¶

Traffic goes through BIG-IP VE to a pool. Your application servers should be members of this pool.

1. Open a web browser and go to the BIG-IP Configuration utility, using the public IP address on the management network, for example: https://<external-ip-address>.
2. On the **Main** tab, click **Local Traffic -> Pools**.
3. Click **Create**.
4. In the **Name** field, type web pool. Names must begin with a letter, be fewer than 63 characters, and can contain only letters, numbers, and the underscore (_) character.
5. For Health Monitors, move https from the **Available** to the **Active** list.
6. Choose the load balancing method or retain the default setting.
7. In the **New Members** section, in the **Address** field, type the IP address of the application server.
8. In the **Service Port** field, type a service port, for example, **443**.
9. Click **Add**. The list now contains the member.
10. Add additional pool members as needed and click **Finished**.

Create a secondary private IP for the VIP¶

In the OCI console, create a secondary private IP on the external NIC.

1. Click the top-left menu and under **Compute**, click **Instances**.
2. Click the name of your instance.
3. In the left menu, click **Attached VNICs**.
4. Click the external VNIC.
5. Click **Assign Private IP Address.**
6. For **Private IP Address**, in this example, type 10.0.1.202.
7. If you want an external IP address for your application, click **Reserved Public IP**.
8. Click **Assign**.

Create a virtual server

You must create a virtual server for the secondary private IP address that's associated with the external network interface. Application traffic goes to the Elastic IP (EIP) address associated with this BIG-IP VE virtual server.

1. In the BIG-IP Configuration utility, on the **Main** tab, click **Local Traffic -> Virtual Servers**.
2. Click **Create** and populate the following fields.

Field	Value
Name	A unique name
Destination Address/Mask	10.0.1.202 (the secondary private IP address on the external NIC)
Service Port	A port number or a service name from the Service Port list
HTTP Profile	http
Source Address Translation	Auto Map
Default Pool	web_pool

3. Configure any other settings as needed and click **Finished**.

Traffic to the virtual server IP address will now go to the pool members.

Deploy BIG-IP B

The second instance of BIG-IP VE is referred to as **BIG-IP B**.

Create a second BIG-IP VE

Now deploy a second BIG-IP VE instance from the custom image you created. Follow the same instructions as the first BIG-IP VE.

We will call this instance **BIG-IP B** and the first instance **BIG-IP A**.

Create VNICs and reboot

You must associate three VNICs with BIG-IP B.

Important: Ensure the BIG-IP VE instance is running.

1. In the OCI console, under the **Compute** section, click **Instances**.
2. Click the name of your instance (BIG-IP B).
3. In the left menu, click **Attached VNICs**.
4. Click **Create VNIC** and complete the fields one time for each VNIC:

Name	Virtual Cloud Network	Subnet	Private IP address	Assign public IP address
External	Your VCN	External	10.0.1.3	Enable
Internal	Your VCN	Internal	10.0.2.3	Disable
HA	Your VCN	HA	10.0.3.3	Disable

5. Click **Create VNIC**.

6. Reboot BIG-IP VE by clicking the instance and clicking **Reboot**, leave the default selection and click **OK**.

Important: You must reboot for BIG-IP VE to recognize the VNICs.

License and Provision BIG-IP B¶

Follow the previous instructions to license and provision BIG-IP B.

- License
- Provision

Create three VLANs on BIG-IP B

In BIG-IP B, you must create an external and internal VLAN that corresponds to the Oracle subnets.

You can use the previous instructions to do this.

Create three self IP addresses¶

1. Click **Create** and populate the appropriate fields for the external self IP address.

Field	Value
Name	ExternalSelfIP
IP Address	10.0.1.3
Netmask	255.255.255.0
VLAN/Tunnel	external
Port Lockdown	Allow All

2. Click **Repeat** and populate the appropriate fields for the internal self IP address.

Field	Value
Name	InternalSelfIP
IP Address	10.0.2.3
Netmask	255.255.255.0
VLAN/Tunnel	internal
Port Lockdown	Allow All

3. Click **Repeat** and populate the appropriate fields for the HA self IP address.

Field	Value
Name	HASelfIP
IP Address	10.0.3.3
Netmask	255.255.255.0
VLAN/Tunnel	HA
Port Lockdown	Allow All

4. Click **Finished**.

The screen refreshes, and the three new self IP addresses are in the list.

Configure High Availability

You must first configure BIG-IP A and B to communicate for the purposes of synchronizing their configurations and failing over.

However, HA will not work until the final step, where you configure scripts to reassign the secondary private IP address (the virtual IP, or VIP). These steps are detailed in the final section of the guide.

Specify config sync, failover, and mirroring addresses¶

Each BIG-IP VE needs to synchronize its configuration with and assess the health of the other BIG-IP VE.

1. Log in to the BIG-IP Configuration utility on **BIG-IP A**.
2. On the Main tab, click **Device Management -> Devices**.
3. In the **Name** column, click **BIG-IP A.**
4. From the **Device Connectivity** menu, choose **ConfigSync**.
5. For the **Local Address** setting, select the static self IP address for **BIG-IP A**'s internal VLAN, 10.0.2.2, and then click **Update**.
6. From the **Device Connectivity** menu, choose **Failover Network**.
7. For the **Failover Unicast Configuration** settings, click **Add** and specify the static self IP address for **BIG-IP A**'s HA VLAN, 10.0.3.2.
8. Click **Finished**.

Now log in to **BIG-IP B**.

1. On the **Main** tab, click **Device Management -> Devices**.
2. In the **Name** column, click **BIG-IP B.**
3. From the **Device Connectivity** menu, choose **ConfigSync**.
4. For the **Local Address** setting, select the static self IP address for **BIG-IP B**'s internal VLAN, 10.0.2.3, and click **Update**.
5. From the **Device Connectivity** menu, choose **Failover Network**.
6. For the **Failover Unicast Configuration** settings, click **Add** and specify the static self IP address for **BIG-IP B**'s HA VLAN, 10.0.3.3.
7. Click **Finished**.

Now each BIG-IP VE can use the IP addresses of the other BIG-IP VE to sync its configuration and fail over.

Establish trust between the BIG-IP VEs¶

Before joining a Sync-Failover device group, both BIG-IP VEs must authenticate each others' certificates to create trust.

Note: Do this task on **BIG-IP A** ONLY.

1. Log in to the BIG-IP Configuration utility on **BIG-IP A**.
2. On the **Main** tab, click **Device Management -> Device Trust**, and then select **Device Trust Members**.
3. Click **Add**.
4. For the IP address, type the management address for **BIG-IP B**, 10.0.0.3.

   This is the primary private IP address associated with **BIG-IP B**'s management subnet.
5. Type the administrative user name and password.
6. Click **Retrieve Device Information**.

   BIG-IP A discovers BIG-IP B and displays information about it. Confirm that BIG-IP B's certificate is correct and click **Device Certificate Matches**.
7. Confirm that **BIG-IP B**'s certificate is correct.
8. Confirm that the management IP address and name of **BIG-IP B** are correct.
9. Click **Device Certificate Matches**.
10. Confirm the name and click **Add Device.**

BIG-IP A and **BIG-IP B** now trust each other. In the top left, the status changes to **In Sync**.

Create a Sync-Failover device group¶

You must put the two BIG-IP-IP VEs into a Sync-Failover device group. If an active BIG-IP VE in the Sync-Failover device group becomes unavailable, its configuration objects fail over to the other BIG-IP VE and traffic processing resumes.

Note: Do this task on **BIG-IP A** only.

1. Log in to the BIG-IP Configuration utility on **BIG-IP A**.
2. On the Main tab, click **Device Management -> Device Groups**.
3. On the **Device Groups** list screen, click **Create**.
4. Type a name for the device group, like bigip_ve_oracle.
5. Select the device group type **Sync-Failover**.
6. In the **Configuration** pane, select both BIG-IP VEs from the **Available** list and click the **Move** button.

   Both BIG-IP VEs appear in the **Includes** list.
7. For the **Sync Type**, leave **Manual with Incremental Sync**.
8. Click **Finished**.

You now have a Sync-Failover device group that contains both BIG-IP VEs.

Sync the BIG-IP configuration to the device group¶

You must synchronize the BIG-IP configuration data from **BIG-IP A** to **BIG-IP B**. This data includes the floating virtual IP address, 10.0.1.202.

Note: Do this task on **BIG-IP A** ONLY.

1. Log in to the BIG-IP Configuration utility on **BIG-IP A**.
2. On the **Main** tab, click **Device Management -> Overview**.
3. In the **Device Groups** pane, from the **Name** column, select the device group you created earlier, such as bigip_ve_oracle.

   The screen expands to show a summary and details of the sync status of the device group, as well as a list of the two BIG-IP VEs within the device group.
4. In the **Devices** pane, in the **Sync Status** column, select the device that shows a sync status of **Changes Pending**. (or **Awaiting Initial Sync**).
5. Click **Sync**.

   This syncs the most recent changes on **BIG-IP A** to the other member of bigip_ve_oracle, **BIG-IP B**. In the top left, one BIG-IP should show **Active** status, and the other, **Standby**.

If you have issues with high availability, check the log messages by using SSH to log in to the BIG-IP VEs. At the system prompt, type the command tail -n 20 /var/log/ltm. This shows the most recent twenty rows of log messages.

Finalize High Availability

Finally, you must customize and deploy scripts that allow BIG-IP VE to communicate with Oracle and move the virtual IP address from one BIG-IP VE to the other.

Create API keys

You need keys for BIG-IP to interact with the Oracle API. You will create the keys locally, and then copy the public key into the OCI console.

1. To generate public and private keys, point your browser to https://docs.cloud.oracle.com/iaas/Content/API/Concepts/apisigningkey.htm#How, and then complete the **Generate an API Signing Key** task. For example:

   When done, you will have two files in a folder named, .**oci**:

   - oci_api_key.pem
   - oci_api_key_public.pem
2. To add the contents of the .pem file to OCI, open the OCI console, and in the top-right corner, next to your username, hover over the down-arrow and click **User Settings**.

3. In the **API Keys** section, click **Add Public Key**, paste the contents of oci_api_key_public.pem file into the box, and then click **Add**.

A Fingerprint is generated.

Copy files from github

Now you are going to copy some files from github, edit them, and copy them to the BIG-IP VE instances.

1. Copy these files from github (https://github.com/f5devcentral/f5-oci-failover) to a local directory where you can edit them.

```
active
oci-curl
vnicext2.json
vnicint2.json
```

2. You will edit these files, and then copy them to the BIG-IP VE instances.

   Alternately, you can copy them to BIG-IP VE now and edit while on the instance. See Copy the files to BIG-IP VE instances for more information on where to copy.

Edit the oci-curl file

You must edit the oci-curl file to have information about your OCI environment.

Specifically, you need values for these four values:

```
local tenancyId="ocid1.tenancy.oc1..ocid1.privateip.oc1.phx.abyhqljREPLACETHISWITHYOUROCIDSa";

local authUserId="ocid1.user.oc1..aaaaaaaaky3iyt7oqbdolpppdnqfbbarbREPLACETHISWITHYOUROCIDSvwq";

local keyFingerprint="b0:77:5f:39:37:36:e2:dc:98:d2:00:00:00:00:00:00";

local privateKeyPath="/config/failover/oci_api_key.pem";
```

To get the tenancyId

1. In the OCI console, at the top of the page, click the tenancy name.
2. Under **Tenancy Information**, next to **OCID**, click **Show**.
3. Copy the value and paste it into the oci-curl file as the **tenancyID** value.

To get the authUserId

1. In the OCI console, in the top-right corner, next to your username, hover over the down arrow and click **User Settings**.
2. In the **User Information** section, next to **OCID**, click **Show**.
3. Copy the value and paste it into the oci-curl file as the **authUserId** value.

To get the keyFingerprint

1. In the top-right corner, next to your username, hover your mouse over the down arrow and click **User Settings**.
2. In the left menu, click **API Keys**.
3. In the **API Keys** section, copy the fingerprint and paste it into the **oci-curl** file as the **keyFingerprint** value.

To get the privateKeyPath

Connect to the BIG-IP VE instance and copy your .pem file into the config/failover folder.

If you used a .pem file other than the one generated by following the Oracle documentation, you may need to update the **privatekeypath** value.

Edit the active file

Open the active file and replace these values.

Replace the region URL

Replace the region URL with the one specific to your region.

1. Go to this web page: https://docs.cloud.oracle.com/iaas/Content/API/Concepts/apiref.htm
2. In the section called **Core Services API (covering Networking, Compute, and Block Volume)**, find the region you're working in, for example: iaas.us-phoenix-1.oraclecloud.com
3. Put this value in the highlighted text in the active file:

```
# External Secondary IP failover
/config/failover/oci-curl iaas.us-phoenix-1.oraclecloud.com PUT
/config/OCI/vnicext2.json
"/20160918/privateIps/ocid1.privateip.oc1.phx.abyhqljREPLACETHISW
ITHYOUROCIDShdy"
```

Replace the OCID for the secondary external private IP address

Find the OCID of the secondary private IP address on the external VNIC:

1. Open OCI console, click the **Main** menu and under **Compute**, click **Instances**.
2. Click the name of your instance.
3. In the left menu, click **Attached VNICs**.
4. Click the name of the **external VNIC**.
5. Look at the secondary private IP address, 10.0.1.202 in this example.
6. Next to the **Private IP OCID**, click **Show**, and then copy the **Public IP OCID** value.

7. Put this value into the highlighted text in the active file:

```
# External Secondary IP failover
/config/failover/oci-curl iaas.us-phoenix-1.oraclecloud.com PUT
/config/OCI/vnicext2.json
"/20160918/privateIps/ocid1.privateip.oc1.phx.abyhqljREPLACETHISW
ITHYOUROCIDShdy"
```

8. Delete this section of the file:

```
# Internal Secondary IP failover
/config/failover/oci-curl console.us-phoenix-1.oraclecloud.com
PUT /config/OCI/vnicint2.json
"/20160918/privateIps/ocid1.privateip.oc1.phx.abyhqljREPLACETHISW
ITHYOUROCIDS5dq"
```

Ensure path to json files is correct

Ensure the path to the json file is /config/failover. In the default script, the value is /config/OCI/vnicint2.json

It must be **/config/failover**, because that is the location where you will copy the files.

Edit the json files

Finally, you must update the json files with the OCID values of the VNICs.

1. Create a copy of the files: **vnicint2.json** and **vnicext2.json**. One copy will go on **BIG-IP A**, and one on **BIG-IP B**.
2. Edit **vnicint2.json** and **vnicext2.json**, according to the BIG-IP VE it applies to.

   BIG-IP 1:

```
vnicint2.json
                OCID of Internal VNIC of BIG-IP 1
vnicext2.json
                OCID of External VNIC of BIG-IP 1
```

   BIG-IP 2:

```
vnicint2.json
                OCID of Internal VNIC of BIG-IP 2

vnicext2.json
                OCID of External VNIC of BIG-IP 2
```

To find these OCIDs:

1. Open OCI console, click the **Main** menu, and under **Compute**, click **Instances**.
2. Click the **name** of the instance.

3. In the left menu, click **Attached VNICs**.
4. Click the name of the **VNIC** and then click **Copy** next to **OCID**.

Copy the files to BIG-IP VE instances

1. Connect to **BIG-IP A** and copy the **active** and **oci-curl** files to the **/config/failover** folder.

   NOTES:

   - These two files should be the same on both BIG-IP VE instances.
   - You are overwriting an existing file named, *active*. If you want to preserve it, then rename it to *active_old*.
2. Connect to **BIG-IP B** and copy the **active** and **oci-curl** files to the **/config/failover** folder.
3. Copy the two .**json** files to each BIG-IP VE instance. These files are specific to each BIG-IP VE.
4. On each BIG-IP VE, set permissions on the **active** and **oci-curl** files so they have *execute* permissions (for example, `chmod +x oci-curl`).
5. On each BIG-IP VE, copy the .pem file from your local .oci folder:
   - Previously, you created a .pem file called **oci_api_key.pem**. Copy this .pem file into the **/config/failover** folder.
   - If you used a .pem file other than the one generated by the following the Oracle documentation, or your .pem file has a different name, open the oci-curl file and ensure the **privatekeypath** reflects the location and name of your file.

Trigger failover

You can now trigger failover.

On the active BIG-IP VE instance, log into the Configuration utility and under **Device Management** -> **Traffic Groups**, select the check box by traffic-group-1 and click **Force to Standby**.

In the OCI console, the secondary private IP address on the external VNIC moves from the standby BIG-IP VE instance to the active one.