



Deploying BIG-IP High Availability Across AWS Availability Zones

Welcome to the F5® deployment guide for configuring the F5 BIG-IP® system Virtual Edition (VE) for high availability across Amazon Web Services (AWS) Availability zones. This guidance is ideal for organizations that want to deploy public, Internet-facing services on a traditional high availability pair of BIG-IP systems, but also leverage the benefits of AWS Availability Zones. This guide also describes how to configure the BIG-IP system to manage AWS routes for your clients and/or applications.

This implementation uses F5's AWS Advanced HA iApp template. iApp is a powerful set of features in the BIG-IP system that provides a new way to architect application delivery in the data center, and it includes a holistic, application-centric view of how applications are managed and delivered inside, outside, and beyond the data center. The AWS Advanced HA iApp acts as a single-point interface for building, managing, and monitoring the deployment. For more information on iApps, see the White Paper F5 iApp: Moving Application Delivery Beyond the Network at <http://www.f5.com/pdf/white-papers/f5-iapp-wp.pdf>

F5 has released an Amazon CloudFormation template on GitHub that greatly simplifies this configuration. For details, see <https://github.com/F5Networks/f5-aws-cloudformation/tree/master/supported/failover/across-net/via-api>.

Products and applicable versions

| Product | Versions |
|---|---|
| BIG-IP Virtual Edition in Amazon Web Services | 12.1.0 HF2 - 13.1.0.2 |
| iApp template | f5.aws_advanced_ha.v1.3.0rc1 and f5.aws_advanced_ha.v1.4.0rc5 |
| Deployment Guide version | 2.2 (see <i>Document Revision History on page 19</i>) |
| Last updated | 05-23-2019 |

Important: Make sure you are using the most recent version of this deployment guide, available at <http://f5.com/pdf/deployment-guides/f5-aws-ha-dg.pdf>.

If you are looking for older versions of this or other deployment guides, check the Deployment Guide Archive tab at: <https://f5.com/solutions/deployment-guides/archive-608>

To provide feedback on this deployment guide or other F5 solution documents, contact us at solutionsfeedback@f5.com.

Contents

| | |
|--|-----------|
| Prerequisites and configuration notes | 3 |
| AWS Prerequisites and general configuration notes | 3 |
| BIG-IP VE prerequisites and general configuration notes | 4 |
| Configuration scenario: HA Cluster across Availability zones | 5 |
| Amazon Web Services initial configuration | 6 |
| Creating an Amazon Virtual Private Cloud with two Availability Zones | 6 |
| Deploying a BIG-IP VE in each Availability Zone | 6 |
| BIG-IP VE initial configuration | 9 |
| Preparing the BIG-IP systems for the Advanced HA across Availability Zones configuration | 9 |
| Configuring the BIG-IP VE in Availability Zone 1 | 10 |
| Configuring a public/external Self IP with Port Lockdown | 10 |
| Creating a new partition | 10 |
| Configuring a default route in the new partition | 10 |
| Switching back to the Common partition | 10 |
| Setting the BIG-IP ConfigSync local address | 11 |
| Configuring the failover network | 11 |
| Configuring the BIG-IP VE in Availability Zone 2 | 11 |
| Completing the clustering configuration on the BIG-IP VE in Availability Zone 1 | 11 |
| Adding the BIG-IP VE in Availability Zone 2 to the Peer List | 11 |
| Creating a Device Group | 12 |
| Enabling Network Failover | 12 |
| Creating BIG-IP virtual servers and associated objects for each Availability Zone | 12 |
| Using the TCP iApp template to configure the virtual servers | 12 |
| Manually creating the virtual servers | 12 |
| Assigning the virtual servers to Traffic Group: None | 13 |
| Preparing for the Route Management configuration | 14 |
| Prerequisites for the Route Management scenario | 14 |
| Running the iApp template | 15 |
| Known Issues | 18 |
| Document Revision History | 19 |

Prerequisites and configuration notes

The following are general prerequisites and configuration notes for this guide:

- **IMPORTANT:** F5 has released a CloudFormation Template (CFT) that automates the configuration described in this guide. This CFT runs this iApp template programmatically, and is supported by F5 Networks. You should only use the procedures in this guide if you want to configure this solution manually.
- We assume you are familiar with the concepts in the following articles on DevCentral:
 - » *F5 in AWS Part 1 - AWS Networking Basics*
<https://devcentral.f5.com/articles/f5-in-aws-part-1-aws-networking-basics>
 - » *F5 in AWS Part 2 - Running BIG-IP in an EC2 Virtual Private Cloud*
<https://devcentral.f5.com/articles/f5-in-aws-part-2-running-big-ip-in-an-ec2-virtual-private-cloud>
 - » *F5 in AWS Part 3 - Advanced Topologies and More on Highly Available Services*
<https://devcentral.f5.com/articles/part-3-of-big-ip-in-ec2-advanced-topologies-and-more-on-highly-available-services>
- There are two distinct scenarios presented in the iApp template: using the BIG-IP system to configure high availability across AWS Availability zones, and using BIG-IP system to manage AWS routes for your clients and/or applications. You can configure one or both options using the iApp template.
- This iApp does not support IPv6.

AWS Prerequisites and general configuration notes

- You must have a minimum of three Elastic IP addresses (EIPs), one for each BIG-IP device's Self IP address and one for a public Internet-facing virtual server.
 - » You must have an additional EIP allocated for each virtual server (or specifically virtual address) on the BIG-IP system you want to be a part of this implementation.
- You must have AWS Access and Secret Keys: for a user with permissions to manage the EIPs.
Note: If you are using an BIG-IP instance of v13.0 or later, the Access and Secret keys are not required, as v13.0 and later support using IAM Roles for authentication.
- The high availability section of the iApp template is not responsible for allocating/de-allocating EIPs or adding/deleting associations. It simply remaps (or "re-associates") existing EIPs. Make sure Secondary Private IPs associated with the BIG-IP Virtual Servers have **Allow Re-Association** attribute checked upon first provisioning.

This setting is found at **EC2 Dashboard -> Network & Security -> Interfaces -> Manage Private IP Addresses**.

- You must have the following roles (at a minimum) in your IAM (Identity and Access Management) policy. For example:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeAddresses",
        "ec2:AssociateAddress",
        "ec2:DisassociateAddress",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeNetworkInterfaceAttributes",
        "ec2:DescribeRouteTables",
        "ec2:ReplaceRoute"
      ],
      "Resource": [
        "*"
      ],
      "Effect": "Allow"
    }
  ]
}
```

BIG-IP VE prerequisites and general configuration notes

- **New** You must be using a BIG-IP VE with 2 or more NICs. Network Failover does not work with a 1 NIC AWS deployment.
- You must be using BIG-IP version 12.1.0 HF2 or later. The iApp is available on downloads.f5.com. See *Downloading and importing the iApp on page 15* for more information.
- F5 has created a number of experimental Cloud Formation Templates for deploying F5 services in Amazon Web Services EC2, available on GitHub at <https://github.com/F5Networks/f5-aws-cloudformation>. The templates with **across-az-cluster** in the name configure the BIG-IP system using this iApp.
- BIG-IP requires that hourly images must have a Public IP assigned in order to license them. To deploy hourly billing on a BIG-IP v12.1 Virtual Edition (VE) in AWS, you must create a key pair and a VPC (if none exists). If using BIG-IP v13.0 or later, this is not required.

Also, when deploying BIG-IP VE, you must ensure that **eth0** (used for management access) can access the Internet. Note that the following steps are required so that BIG-IP VE can be licensed with F5 when it boots when using version 12.1 and beyond. If desired, you can remove these public IP addresses after the instance is licensed).

Ensuring that **eth0** can access the Internet can be achieved by one of the following:

- » Putting **eth0** in a subnet with an Internet Gateway
 - » Associating a public IP to a BIG-IP VE management IP (**eth0**). Associate an Elastic IP to the management NIC within a few minutes of deployment, or associate it later and restart the instance.
- While this guide shows you how to instantiate a BIG-IP VE virtual appliance in AWS, it does not provide specific instructions for the initial configuration of the BIG-IP device (including creating a key pair, licensing the devices, setting admin and root passwords, and configuring VLANs). See the BIG-IP documentation if you need assistance with these tasks: https://support.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/bigip-ve-setup-amazon-ec2-12-0-0/3.html

 **Warning** *The BIG-IP Management Interface should never be exposed to the Internet (i.e. via a Public IP or EIP). Access it instead through other methods like a VPN, Direct Connect network, secured jumpbox, etc.*

- DHCP must be disabled. BIG-IP VEs use DHCP by default but Device Service Clustering does not currently support DHCP. The BIG-IP section has specific details on configuring this option.
- This solution currently supports the following modules only: LTM, ASM, AFM and Analytics. While you may use these modules in your environment, the iApp template does not configure any ASM, AFM, or AVR objects. It is outside the scope of this document to provide specific configuration guidance for these modules. See the appropriate product documentation.
- Connection and Persistence mirroring on the BIG-IP system are not supported.
- If you require SNAT, this solution only supports using SNAT Auto Map.
- You can only have one instance of the iApp template running at a time.
- Clustering is restricted to HA pairs.
- Most of the configuration in this guide is performed from the BIG-IP Configuration utility.
- Because subnets/address space are different in each Availability Zone, you cannot have floating IP addresses. The BIG-IP configuration section has specific details.

Configuration scenario: HA Cluster across Availability zones

Unlike the traditional High Availability (HA) within a Single Availability Zone (AZ) deployment, where Active status dictates ownership of floating virtual addresses within the same subnet, here Active status dictates ownership of Elastic IPs (EIPs). However, similar to a Single Availability Zone deployment, one of the benefits of this deployment is that it does not require DNS LB (GSLB) for public Internet-facing virtual servers. This makes it ideal for applications or firewall issues where static IPs are required.

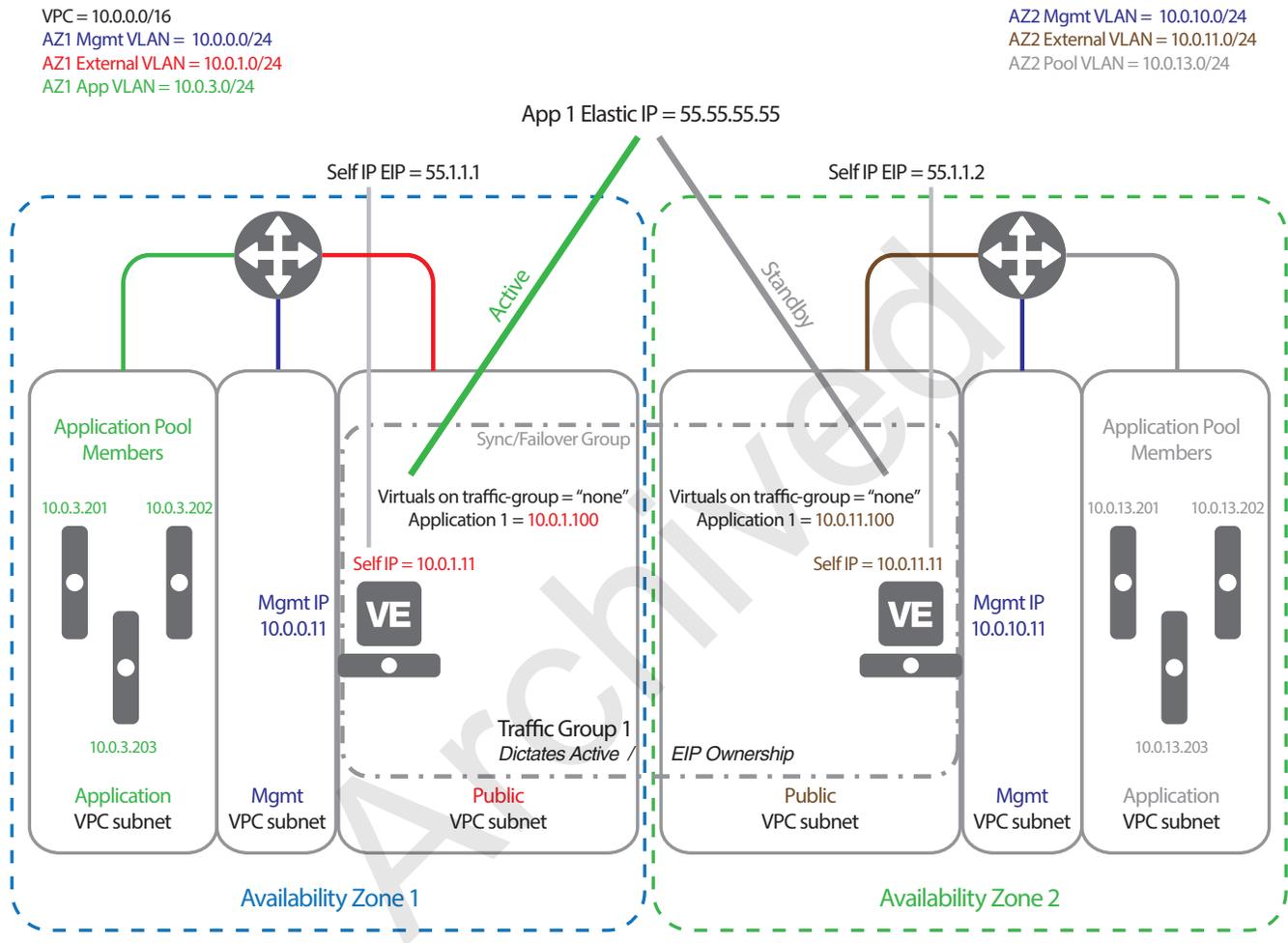


Figure 1: Configuration example

This guide contains the following major sections:

- Amazon Web Services initial configuration on page 6
- BIG-IP VE initial configuration on page 9
- Running the iApp template on page 15

The tasks you perform in the BIG-IP VE initial configuration depend on whether you are deploying high availability across Availability Zones, route management, or both.

Amazon Web Services initial configuration

In this section, we provide guidance on the initial AWS configuration, including deploying a BIG-IP VE in each Availability Zone. If you already have already completed these tasks, continue with *Preparing the BIG-IP systems for the Advanced HA across Availability Zones configuration on page 9*.

Creating an Amazon Virtual Private Cloud with two Availability Zones

The first task is to create a Virtual Private Cloud (VPC) with two Availability Zones. It is outside the scope of this document to provide specific instructions for the Amazon configuration, and Amazon does an excellent job of documenting how to configure a VPC and Availability Zones on their website. See <https://aws.amazon.com/documentation/vpc/>.

Ensure you configure two Availability Zones.

Deploying a BIG-IP VE in each Availability Zone

The next task is to deploy a BIG-IP VE virtual appliance in each Availability Zone.

This section contains an overview of the tasks for deploying the BIG-IP VE in each Availability Zone. For complete instructions, we recommend you see the **BIG-IP Virtual Edition Setup Guide for Amazon EC2** available on Ask F5: https://support.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/bigip-ve-setup-amazon-ec2-12-0-0.html.

To deploy a BIG-IP VE in an AWS Availability zone

1. Log in to your account on Amazon Web Services (AWS) marketplace.
2. In the Search AWS Marketplace bar, type **F5 BIG-IP** and then click **GO**. The F5 BIG-IP Virtual Edition for AWS option is displays.
3. Click F5 BIG-IP Virtual Edition for AWS (BYOL) and then click **Continue**.
4. Click the Launch with EC2 Console tab.
5. Select the BIG-IP software version appropriate for your installation and then click the Launch with EC2 button that corresponds to the Region that provides the resources you plan to use.
6. Select an **Instance Type** appropriate for your implementation.
7. In the **Configure Instance** section, configure the Network Interfaces.

Important Make sure two Network Interfaces are attached (*eth0* for the mgmt subnet and *eth1* for the public/external subnet) before the initial boot. A single Network Interface deployment is not supported. If launching manually, hit "Add Device" before launch so you have *eth1*: .

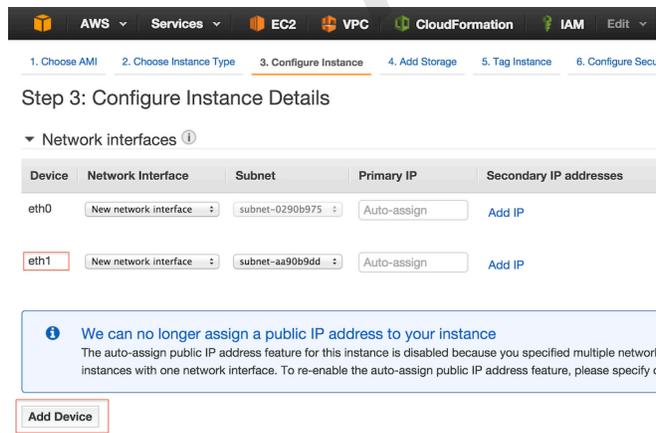


Figure 2: Configuring the Instance details

8. Create an IAM role and then attach a policy to the role with the following policy document:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeAddresses",
        "ec2:AssociateAddress",
        "ec2:DisassociateAddress",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeNetworkInterfaceAttributes",
        "ec2:DescribeRouteTables",
        "ec2:ReplaceRoute",
        "ec2:assignprivateipaddresses"
      ],
      "Resource": [
        "*"
      ],
      "Effect": "Allow"
    }
  ]
}
```

9. Create **Security Groups** using the following guidance. If you have an existing BIG-IP, the Security Group for the Management interface needs to have the following rules:

 **Note** *If launching BIG-IP VEs through the Console (via the Launch Instance Wizard), TCP 22 and 443 are a good start for an initial Mgmt Port Security Group. Adding additional rules (like ICMP shown in the following example) are optional but may be helpful. Give the group a more generic name (such as BIG-IP-Mgmt-Int-Security-Group) so it can be reused on the peer, and make sure to lock down the Source Addresses.*

- **Management Interface:**
 - » TCP 22 = SSH/SCP (Source = Intra-VPC and/or mgmt networks)
 - » TCP 443 = HTTPS (Source = Intra-VPC and/or mgmt networks)
 - » ICMP ALL = (Source = Intra-VPC and/or mgmt networks)

 **Warning** *The Management Interface should never be exposed to the Internet (i.e. via a Public IP or EIP). Access it instead through other methods such as a VPN, Direct Connect network, secured jumpbox, and the like.*

Configure Additional Security Rules for the public facing interface. If you have an existing BIG-IP, the Security Group for the Public/External interface needs to have the following rules:

- **HA-Channel (eth1):**
 - » UDP 1026 = Failover Heartbeat (Source = Intra-VPC or Peer's Public subnet)
 - » TCP 4353 = ConfigSync (Source = Intra-VPC or Peer's Public subnet)
 - » ICMP ALL = (Source = Intra-VPC and/or mgmt networks)
- **Virtual Server Traffic (eth1):**
 - » Allow 80/443 = HTTP/HTTPS or any other port serving virtual server traffic (Source = Any). See Figure 3.

Create Security Group

Security group name: BIG-IP Public Interfaces

Description:

VPC: vpc-bc2223d9 (10.0.0.0/16) | HA-Across-AZ

Security group rules:

| Type | Protocol | Port Range | Source |
|-----------------|----------|------------|------------------------|
| Custom TCP Rule | TCP | 4353 | Custom IP: 10.0.0.0/16 |
| Custom UDP Rule | UDP | 1026 | Custom IP: 10.0.0.0/16 |
| All ICMP | ICMP | 0 - 65535 | Custom IP: 10.0.0.0/16 |
| HTTPS | TCP | 443 | Anywhere: 0.0.0.0/0 |
| HTTP | TCP | 80 | Anywhere: 0.0.0.0/0 |

Buttons: Add Rule, Cancel, Create

Figure 3: AWS Security Group configuration

Warning As the public interface has 443 open to the Internet, make use the **Port Lockdown** list on the Self IPs and/or AFM rules to only the HA-Communication Ports (TCP 4353 and UDP 1026) to avoid exposing the BIG-IP's MGMT host (GUI and SSH). This Port Lockdown configuration is described in the BIG-IP Self IP address configuration.

Note Similar to all BIG-IP AWS deployments, use the ENI's Primary IP for the BIG-IP system's unique Self IP and allocate additional "Secondary Private IPs" for each of your respective virtual servers.

Go to EC2 Dashboard > Network & Security > Network Interfaces > Select the ENI associated with your Public ENI > Manage Private IP Addresses > Assign New IP

For more information, see AskF5 and/or DevCentral articles mentioned in the prerequisites.

This completes the configuration in this section. Again, for specific, step-by-step instructions on deploying the BIG-IP system in AWS, see https://support.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/bigip-ve-setup-amazon-ec2-12-0-0.html

BIG-IP VE initial configuration

This section contains guidance on items you must configure on the BIG-IP VE before you run the iApp template.

The requirements depend on which of the scenarios you are planning to deploy. If you plan to deploy the system for both high availability across Availability Zones and Route Management, complete both sections.

- *Preparing the BIG-IP systems for the Advanced HA across Availability Zones configuration, on this page*
- *Preparing for the Route Management configuration on page 14*

Preparing the BIG-IP systems for the Advanced HA across Availability Zones configuration

Before you can use the iApp template for configuring high availability across AWS Availability Zones, you must ensure the BIG-IP systems are configured properly.

Note *If you already have BIG-IP systems in your AWS deployment, you may have some of these objects already created. In the following procedures, we note the specific settings you must configure for this implementation for existing objects.*

Prerequisites for the HA across Availability Zones section

- As stated in the prerequisites on page 3, this guide does not provide specific instructions for the initial configuration of the BIG-IP device (including creating a key pair, licensing the devices, setting admin and root passwords, and configuring VLANs). See the BIG-IP documentation if you need assistance with these tasks.
- **Important: No floating addresses**
Because subnets/address space are different in each Availability Zone, you cannot use floating IP addresses. The only traffic-group (which typically contains floating addresses) that should exist is the default traffic-group-1. The presence of this traffic-group determines which BIG-IP is active.

Note *If BIG-IP systems are used to manage outbound traffic, the only address traffic-group-1 might have is a wildcard (0.0.0.0) address used for a forwarding virtual server.*

The lack of floating addresses has implications on the BIG-IP system's SNAT (Source Network Address Translation) functionality. If using SNAT on the virtual servers (i.e. the BIG-IP systems are not the default gateway/route for your application servers), SNAT Auto Map is the only supported SNAT method. SNAT Auto Map uses the unique Self IP of each BIG-IP system for the source address (vs. the traditional floating Self IP).

If NOT using SNAT, you need the BIG-IP systems to be the default gateway/route for your applications. In this case, you need to configure Route Management (*Preparing for the Route Management configuration on page 14*).

For information about SNAT Auto Map, see: <https://support.f5.com/kb/en-us/solutions/public/7000/300/sol7336.html>.

- Your AWS Access and Secret Keys are configured on the BIG-IP system. If they are not, from the BIG-IP Configuration utility, go to **System > Configuration > AWS > Global Settings** and enter the **Access Key** and **Secret Key**.
- DHCP must be disabled on the Management Port. BIG-IP Virtual Editions use DHCP by default, but Device Service Clustering does not currently support DHCP. To check your DHCP configuration, go to **System > Platform > Management Port Configuration**. If necessary, click the **Manual** button.
- *Pool Members must be routed*
As shown in the *Figure 1: Configuration example on page 5*, your pool members (application/web servers) must also be routed (not be on any directly connected subnets as the BIG-IP system). All traffic to pool members should go out through the default gateway (which in AWS is typically the Internet Gateway (IGW)). This requirement ensures traffic flows in a similar and predictable manner on both BIG-IP systems.
- You must have DNS (**System > Configuration > Device > DNS**) and NTP (**System > Configuration > Device > NTP**) configured on the BIG-IP systems.

This section contains the following tasks:

- [Configuring the BIG-IP VE in Availability Zone 1 on page 10](#)
- [Configuring the BIG-IP VE in Availability Zone 2 on page 11](#)
- [Completing the clustering configuration on the BIG-IP VE in Availability Zone 1 on page 11](#)
- [Creating BIG-IP virtual servers and associated objects for each Availability Zone on page 12](#)

Configuring the BIG-IP VE in Availability Zone 1

Use the following guidance to configure the BIG-IP VE in Availability Zone 1. The following sections contain tables with guidance on configuring required BIG-IP objects. The header of each table shows the path to the object and assumes you are looking at the Main tab of the BIG-IP Configuration utility. For specific instructions or help configuring this objects, see the Help tab or the BIG-IP documentation.

Configuring a public/external Self IP with Port Lockdown

The first task is to create a Self IP address on the public/external VLAN. If you have already created the appropriate Self IP address, use the Port Lockdown guidance in the following table to modify your Self IP appropriately.

| Self IP Port Lockdown (Network > Self IPs) | |
|--|--|
| Name | Type a unique name |
| IP address | Type the appropriate IP address, such as 10.0.1.11 |
| Netmask | Type the appropriate Netmask, such as 255.255.255.0 |
| VLAN/Tunnel | Select your public/external VLAN. |
| Port Lockdown | Select Allow Custom |
| Custom List | Click TCP and then Port . Type 4353 in the Port box and then click Add . Port 4353 is for configsync. Click UDP and then Port . Type 1026 in the Port box and then click Add . Port 1026 is for the failover heartbeat. |

Creating a new partition

The next task is to create a new, local only partition.

| Partition (System > Users > Partition list) | |
|---|--|
| Partition Name | Type a unique name, such as LOCAL_ONLY . |
| Device Group | In the Device Group area, <u>clear the check</u> from the Inherit Device Group from root folder box. If necessary, from the list, select None . |
| Traffic Group | From the Traffic Group list, select traffic-group-local-only (non-floating) . |

After you create the new partition, you must select the new partition you just created from the **Partition** list in the upper right corner of the screen.

Configuring a default route in the new partition

Next, you create a new route in the partition you just created.

 **Critical** Before you configure the default route, you must select the local only partition you just created from the **Partition** list in the upper right corner of the BIG-IP user interface (**LOCAL_ONLY** in our example).

| Routes (Network > Routes > New Route) | |
|--|---|
| Be sure you have selected the Partition you just created from the Partition list before creating this route. | |
| Name | Type a unique name |
| Destination | 0.0.0.0 |
| Netmask | 0.0.0.0 |
| Resource | Use Gateway |
| Gateway Address | Type the gateway address, which is .1 of the public subnet (eth1) you created in AWS, such as 10.0.0.1 |

Switching back to the Common partition

After you create the default route in the new partition, you **must** switch back to the **Common** partition. From the **Partition** list, select **Common**.

Setting the BIG-IP ConfigSync local address

The next task is to select the external self IP with port lockdown you created. Be sure you have changed the Partition back to Common before performing this task.

1. Click **Device Management > Devices**.
2. From the Device List, click the device you are currently configuring.
3. On the Menu bar, click **Device Connectivity > ConfigSync**.
4. From the **Local Address** list, select the Self IP address you configured in *Configuring a public/external Self IP with Port Lockdown on page 10*.
5. Click **Update**.

Configuring the failover network

The next task is to configure the Failover Unicast setting.

1. On the Menu bar, click **Device Connectivity > Failover Network** (if you are not configuring this task immediately after the previous procedure, first follow steps 1 and 2 above).
2. In the Failover Unicast Configuration area, click **Add**.
3. From the **Address** list, select the Self IP address you configured in *Configuring a public/external Self IP with Port Lockdown on page 10*.
4. In the **Port** field, make sure **1026** is the value for the port.
5. Click **Finished**.

This completes the initial configuration of the BIG-IP VE in Availability Zone 1. The next task is to configure the BIG-IP in Availability Zone 2 before returning to this system.

Configuring the BIG-IP VE in Availability Zone 2

The next task is to configure the BIG-IP system in the second Availability Zone.

To configure the second BIG-IP system, simply return to *Configuring a public/external Self IP with Port Lockdown on page 10* and use the same procedures to configure the BIG-IP in Availability Zone 2. Use information appropriate for Availability Zone 2.

Use *Figure 1: Configuration example on page 5* for guidance on configuring the BIG-IP in Availability Zone 2.

Completing the clustering configuration on the BIG-IP VE in Availability Zone 1

The final task in this part of the BIG-IP configuration is to return to the BIG-IP system in Availability Zone 1 and finish the device clustering configuration.

i Important You must have both BIG-IP systems configured as described in this section before performing this step.

Adding the BIG-IP VE in Availability Zone 2 to the Peer List

First, you must add the BIG-IP device in Availability Zone 2 to the Peer List of the BIG-IP in Availability Zone 1.

| Peer List (Device Management > Device Trust > Peer list (on the Menu bar)) | |
|--|---|
| Device IP Address | Type the Management IP address of the BIG-IP in Availability Zone 2. |
| Administrator Username | Type the Administrator Username for the BIG-IP in Availability Zone 2 |
| Administrator Password | Type the password associated with the username. |
| | Click Retrieve Device Information , and then click Finished . |

Creating a Device Group

Next, you create a BIG-IP Device Group and add both BIG-IP devices to it.

| Device Group (<i>Device Management > Device Groups</i>) | |
|--|---|
| Name | Type a unique name such as <code>my_sync_failover_group</code> . |
| Group Type | Sync-Failover |
| Members | From the Available list, select both the BIG-IP in Availability Zone 1 and the BIG-IP in Availability Zone 2, and then click the Add (<<) button. |
| Automatic Sync | Check the box to enable Automatic Sync. |

Enabling Network Failover

The final task in this section is to enable network failover on the device group you just created.

1. Click **Device Management > Device Groups**.
2. From the Device Group list, click the device group you just created.
3. On the Menu bar, click **Failover**.
4. In the **Network Failover** area, click the box to enable Network Failover.
5. Leave the **Link Down Time on Failover** setting at **0.0**.
6. Click **Update**.

Creating BIG-IP virtual servers and associated objects for each Availability Zone

Because subnets in AWS do not span Availability Zones, you must create a virtual server for each zone.

You can either create the virtual servers manually, or you can use the TCP iApp that creates the two virtual servers stored under the single iApp instance.

If you already have virtual servers for each Availability Zone, go to *Assigning the virtual servers to Traffic Group: None on page 13*.

Using the TCP iApp template to configure the virtual servers

To use the TCP iApp, see <https://devcentral.f5.com/codeshare/tcp-iapp-template>. The iApp template recognizes if you run the iApp in AWS, and presents two additional questions asking about the virtual server address you want to use for the other Availability Zone. For assistance using the iApp, see the inline help. The iApp creates two virtual servers, identical except for the IP address (and potentially the IP mask). If you use the iApp template, the system configures one BIG-IP pool which contains members from both or multiple Availability Zones. If you want to use dedicated pools, you must manually configure the system, or run the iApp template twice.

i Important *If you use the iApp template to create the virtual servers, from the Template Selection list at the very top of the template, select Advanced. From the Traffic Group area, clear the check from the Inherit traffic group from current partition/path box, and then select None from the list.*

Manually creating the virtual servers

If you do not want to use the TCP iApp template, you can manually create the virtual servers. It is outside the scope of this document to detail virtual server creation. For assistance on configuring the appropriate objects, see one of the F5 deployment guides (<https://f5.com/solutions/deployment-guides>) or the BIG-IP documentation for creating a virtual server.

If you manually configure the BIG-IP virtual servers, we recommend you create two virtual servers, identical (and referencing the same load balancing pool) except for the IP address (and IP mask if using a network virtual server).

➡ Note *The virtual server for each Availability Zone does not need to have its own Availability Zone-specific pool. The pool can be shared by both virtual servers and contain members for both or multiple Availability Zones.*

After creating the virtual servers, you must assign the virtual addresses to **Traffic Group None** as described in the next section.

Assigning the virtual servers to Traffic Group: None

If you have existing virtual servers you are using for this implementation, you must assign the virtual servers to the special "Traffic Group None". This traffic group allows the virtual servers to accept traffic regardless of the Active/Standby status.

Note *If the Standby BIG-IP system is healthy and somehow receives the traffic on the virtual server associated with its Availability Zone (for example, if the EIP re-mapping failed), it processes the traffic regardless. In this deployment, the Active vs. Standby status simply dictates BIG-IP system to which the EIPs are actively mapped.*

If you manually configured the virtual servers

1. From the Configuration utility, click **Virtual Servers > Virtual Address List**.
2. From the list, click the applicable IP address.
3. From the **Traffic Group** list, select **None**.
4. Click **Update**.
5. Repeat this procedure for all virtual servers that are a part of this implementation.

If you used the iApp template

If you used an iApp template (such as the TCP iApp) to configure your virtual server, you must re-enter the template and modify the Traffic Group information.

1. From the Configuration utility, click **iApps > Application Services > Name of the application service**.
2. On the Menu bar, click **Reconfigure**.
3. From the **Traffic Group** list, uncheck the **Inherit traffic group from current partition/path** box, and then from the list, select **None**.
4. Click **Update**.
5. Repeat this procedure if necessary.

This completes the preparations for the high availability across Availability Zones configuration. If you plan to configure Route Management, continue with the next page. If not, continue with *Running the iApp template on page 15*.

Preparing for the Route Management configuration

This section contains information and prerequisites for using the iApp template to own routes for your clients and/or applications. Using the Route Management option enables traditional BIG-IP HA pairs to perform basic route management of AWS route tables (whether you are in a single Availability Zone or using two Availability Zones as described in this guide).

By having the active BIG-IP take ownership of your client's or application's default or specific routes:

- The BIG-IP virtual servers do not have to use SNAT
- You can manage access traffic (for example, you can point clients/servers to BIG-IP APM VPN for specific on-prem networks)
- You can facilitate various outbound proxy use cases (NAT, URI filtering, and so on).

If you are not configuring Route Management, you can continue with *Running the iApp template on page 15*.

Prerequisites for the Route Management scenario

- You must have AWS Access/Secure Keys, with permissions to query/modify route tables.
- Route tables you modify should not contain any subnets used by BIG-IP systems themselves.
- A route can only point to one ENI at a time, so this only works on an Active/Standby BIG-IP HA cluster, regardless if the cluster members are in the same Availability Zone (Availability Zone) or spread across Availability Zones.
- The Source/Destination check on interfaces in AWS must be disabled on the BIG-IP's ENI's as seen in the following image. A route can only point to one ENI at a time so this only works on an Active/Standby cluster, regardless if the cluster members are in the same Availability Zone or spread across Availability Zones. For instructions, see the AWS documentation.

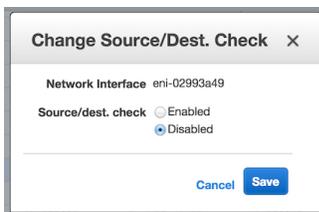


Figure 4: Changing the Source/Destination Check in AWS

- Before running the iApp template, you should have the appropriate Route Table IDs, subnets, and destination CIDR block strings for the subnet that you want the BIG-IP cluster to own ready.
- **IMPORTANT:** Similar to the EIP Mappings described in the previous section, the iApp itself is not responsible for allocating/de-allocating Route Tables or creating/deleting route entries within those tables. It simply modifies the destination/interface to which the routes point.
- If the virtual servers are not using Source Address Translation (SNAT), Source Address Translation should be set to **None**.
- If using the BIG-IP system for outbound traffic, create IP Forwarding virtual servers, using the following guidance:

| Virtual Servers (Local Traffic > Virtual Servers) | |
|---|---|
| Name | Type a unique name. |
| Type | Forwarding (IP) |
| Source Address | Type 10.0.0.0/16 |
| Destination Address | Type 0.0.0.0/0 |
| Service Port | All Ports |
| VLAN and Tunnel Traffic | Select Enabled on and then select your External VLAN and move it to the Selected box. |
| Source Address Translation | Auto Map |

For more information on forwarding virtual servers, see SOL7595: Overview of IP forwarding virtual servers (<https://support.f5.com/kb/en-us/solutions/public/7000/500/sol7595.html>) and SOL14163: Overview of BIG-IP virtual server types (<https://support.f5.com/kb/en-us/solutions/public/14000/100/sol14163.html>).

NOTE: If you have deployed a BIG-IP HA pair across two Availability Zones, this will SNAT outbound traffic to the BIG-IP's unique Self IPs and hence be translated to their associated EIP.

Continue with the next section for guidance on running the iApp template, and specifically see *Route Management on page 16*.

Running the iApp template

The final requirement is to download and run the AWS Advanced HA iApp. Use the following guidance to help configure the BIG-IP VE for HA across Availability Zones and/or Route Management using the BIG-IP iApp template.

Downloading and importing the iApp

The first task is to download and import the iApp template. We recommend using the latest version available on downloads.f5.com (you must be using BIG-IP version 12.1.0 HF2 or later to use iApp version v1.2.0rc1 or later).

To download and import the iApp

1. Open a web browser and go to downloads.f5.com.
2. Click **Find a Download**.
3. In the **BIG-IP F5 Product Family** section, click **iApp Templates**.
4. On the Product Version and Container page, click **iApp-Templates**.
5. Accept the EULA, and then download the iapps zip file to a location accessible from your BIG-IP system.
6. Extract (unzip) **f5.aws_advanced_ha.v<latest version>.tmpl**, found in the **Amazon > AWS_Advanced_HA > Release_Candidates** directory of the zip file.
7. Log on to the BIG-IP system web-based Configuration utility.
8. On the Main tab, expand **iApp**, and then click **Templates**.
9. Click the **Import** button on the right side of the screen.
10. Click a check in the **Overwrite Existing Templates** box.
11. Click the **Browse** button, and then browse to the location you saved the iApp file.
12. Click the **Upload** button. The iApp is now available for use.

Getting Started with the iApp

To begin the iApp Template, use the following procedure.

1. Log on to the BIG-IP system.
2. On the Main tab, expand **iApps**, and then click **Application Services**.
3. Click **Create**. The Template Selection page opens.
4. In the **Name** box, type a name. In our example, we use **aws_ha**.
5. From the **Template** list, select **f5.aws_advanced_ha.v<latest version>**. The template opens.

Advanced options

If you select **Advanced** from the **Template Selection** list at the top of the page, you see Device and Traffic Group options for the application. This feature is a part of the Device Management configuration. This functionality extends the existing High Availability infrastructure and allows for clustering, granular control of configuration synchronization and granular control of failover. To use the Device and Traffic Group features, you must have already configured Device and Traffic Groups before running the iApp. For more information on Device Management, see the product documentation.

1. **Device Group**
For this deployment, leave the Device Group set to the default.
2. **Traffic Group**
For this deployment, leave the Traffic Group set to the default.

Template options

This section contains general template questions.

1. Do you want to see inline help?

Choose whether you want to see informational and help messages inline throughout the template. If you are unsure, we recommend leaving the default, **Show inline help text**. Important notes and warnings are always shown, no matter which selection you make.

- **Yes, show inline help**

This selection causes inline help to be shown for most questions in the template.

- **No, do not show inline help**

If you are familiar with this iApp or with the BIG-IP system in general, you can select this option to hide the inline help text.

2. Do you want to log debug messages?

Choose whether you want the BIG-IP system to log debug messages. By default, important messages are always logged. This option enables additional logging that can assist in debugging any issues that might arise. You can find logs on the BIG-IP system at `/var/log/ltn`.

- **No, do not log debug messages**

Select this option if you do not want to enable debug messages.

- **Yes, log debug messages**

Select this option if you want the system to log debug messages. Again, logs are found on the BIG-IP system at `/var/log/ltn`.

HA Across AZs

This section of the iApp contains guidance on configuring high availability across AWS Availability Zones. You must have already completed all the prerequisite tasks as described in this guide before configuring high availability using this iApp.

1. Would you like to configure high availability for Internet-facing services across Availability Zones?

Choose whether you want to configure high availability across Availability Zones at this time. You must already have created the BIG-IP virtual servers as described in this guide. If you select Yes, the iApp maps Elastic IPs (EIPs) to the virtual addresses associated with those virtual servers. A virtual address can only be mapped to one EIP. Currently, only the following modules are supported for this implementation: LTM, ASM, AFM and Analytics(AVR).

- **No, do not configure high availability across Availability Zones**

Select this option if you do not want to configure high availability across Availability Zones at this time. You can always re-enter the template at a later time to configure this option.

- **Yes, configure high availability across Availability Zones**

Select this option if you want to configure high availability across Availability Zones at this time. To complete this section, you need the AWS Elastic IP address to which you want to map the virtual servers.

- a. Which Elastic IPs should be mapped to BIG-IP virtual addresses?

This part of the template maps the Elastic IP addresses to the virtual servers you created. In the **Elastic IP** field, type the IP address of the Elastic IP address you want to use. From the **AZ1 VIP** and **AZ2 VIP**, select the appropriate virtual server IP addresses you created.

If the BIG-IP virtual server addresses you want to map do not appear in the list, return to *Preparing the BIG-IP systems for the Advanced HA across Availability Zones configuration on page 9* and make sure you have performed all of the prerequisite steps.

Click **Add** to perform additional mappings at this time.

Route Management

In this section, you can configure the BIG-IP system to own routes for your clients and/or applications. See *Preparing for the Route Management configuration on page 14* for more details and prerequisites.

1. Would you like to configure this BIG-IP cluster to own AWS routes?

Choose whether you want the BIG-IP system to own AWS routes at this time.

- **No, do not configure this BIG-IP cluster to own AWS routes**

Select this option if you do not want to configure route management at this time. You can always re-enter the template at a later time to configure this option.

- **Yes, configure this cluster to own AWS routes**

Select this option if you want to configure route management at this time.

- a. Which routes should the BIG-IP cluster own?

In these fields, you enter the routes the Active BIG-IP in the cluster should own.

In the **Route Table ID** field, type the Route Table ID (for example: **rtb-80fae8e5**) that contains the associated subnet. In the **DST CIDR block** field, type the destination CIDR block string for that subnet (for example **0.0.0.0/0**, **172.16.4.0/24**, etc.). You may enter the same route table multiple times if necessary. For instance, if you have two subnets in the same route table.

- b. Which BIG-IP interface should be the gateway?

Select the interface that corresponds to the BIG-IP's ENI to which you would like routes to point.

Finished

Review the information you entered into the template. When you are satisfied that everything is correct, click the **Finished** button and then continue with the next section.

Opening the iApp on the other BIG-IP device

The final task in this configuration is simply to open the iApp template on the BIG-IP system in Availability Zone 2, and then click **Finished**.

 **Critical** You must perform this task at least once to install the failover script. After that, you may update the iApp as usual, on either device.

1. Click **iApps > Application Services**.
2. Click the name of iApp you created.
3. On the Menu bar, click **Reconfigure**.
4. Without making any modifications, at the bottom of the template, click **Finished**.

 **Note:** You must also perform this task whenever you update the iApp template to a new version.

Known Issues

The following are known issues for the configuration described in this guide.

➤ Resetting config to default error

If you try to use the command `tmsh load sys config default`, you may receive an error similar to the following:

```
err tmsh[11858]: 01420006:3: 01020036:3: "The requested application instance (/Common/my_iapp_instance.app/my_iapp) was not found The requested application instance (/Common/my_iapp_instance.app/my_iapp_instance) was not found
```

Workaround:

Delete references to the AWS Advanced HA iApp in the `/config/failover/active` script first before issuing the `tmsh load sys config default` command.

Remove the line containing `python /config/failover/aws_advanced_failover.py`. For example, you can use the following command:

```
[admin@bigip-01-AZ1:Active:In Sync] config # cd /config/failover
[admin@bigip-01-AZ1:Active:In Sync] failover # sed -i.bak '/aws/d' active
```

➤ If using network virtual servers, the built-in same-Availability Zone failover script gives an error

If your configuration uses network virtual servers, you receive an error similar to the following: "

```
err logger: /usr/libexec/aws/aws-failover-tgactive.sh (traffic-group-1): Failed to reassign address: any on interface.
```

Workaround:

If this is a Cluster Across Availability Zone deployment, you can safely ignore as message applies only to same-Availability Zone failover deployments.

If this is a same Availability Zone deployment and only using the Route-Management section, upgrade to a BIG-IP version w/ BZID 484733: `aws-failover-tgactive.sh` doesn't skip network forwarding virtual servers which will instead log an informational message instead:

```
info logger: /usr/libexec/aws/aws-failover-tgactive.sh (traffic-group-1) : IP Address specified during HA takeover is not assigned to any interface. instance-id: i-a95e2c1f. IP address: any
```

```
info logger: /usr/libexec/aws/aws-failover-tgactive.sh (traffic-group-1) : IP Address specified during HA takeover is not assigned to any interface. instance-id: i-a95e2c1f. IP address: 52.0.0.0
```

Document Revision History

| Version | Description | Date |
|---------|---|------------|
| 1.0 | New deployment guide for Advanced High Availability Across AWS Availability Zones. | 03-24-2016 |
| 1.1 | - Added two new prerequisites (marked with a "new" icon) to <i>Prerequisites and configuration notes on page 3</i> - Added support for BIG-IP v12.1 | 09-08-2016 |
| 1.2 | - Added detail to the v12.1 hourly image prerequisite (the first entry in <i>BIG-IP VE prerequisites and general configuration notes on page 4</i>). | 09-13-2016 |
| 1.3 | - Added release candidate v1.2.0rc1 iApp to this guide. There were no visible changes to this version, however there were further checks and support added for AWS EIP ownership. - Added a note to the prerequisites that you must be using BIG-IP version 12.1.0 HF2 to use iApp v1.2.0rc1. | 09-26-2016 |
| 1.4 | - Added the official release candidate v1.2.0rc1 iApp available on downloads.f5.com to this guide. There were no visible presentation changes to this version, but it puts this iApp on the path to full F5 support. | 10-18-2016 |
| 1.5 | - Updated this guide for v1.3.0rc1 of the iApp available on downloads.f5.com. This version contains the following changes: - Added an important note announcing the release of the CloudFormation template on GitHub. This template automates the manual configuration described in this guide. - Added support for BIG-IP version 13.0, and noted v13.0 and later support using IAM roles for authentication. BIG-IP v12.1 and later still require using key and secret authentication. - The supporting scripts used by the iApp have been modified to support IAM roles. - Removed the appendix with TMSH commands from this guide. This configuration is provided by the CFT. | 03-29-2017 |
| 1.6 | Updated this guide for v1.4.0rc1 of the iApp available on downloads.f5.com in the Release_Candidates directory. (note this is the next iApp template release after v1.3.0rc1). This version of the template only contains one change: removed the dependency in the iApp for the AWS EC2 tools SDK in BIG-IP v13.0 and later (BIG-IP v13.0 and later use the AWS CLI SDK). Prior BIG-IP versions still use the EC2 tools SDK. There were no changes to the iApp presentation or this guide. | 05-11-2017 |
| 1.7 | Updated this guide for v1.4.0rc2 of the iApp available on downloads.f5.com in the Release_Candidates directory. This version of the template contains no visible changes to the iApp presentation, and only one change: Corrected an issue in the iApp where in certain situations, the standby unit could own the EIPs after a failover. | 02-01-2018 |
| 1.8 | Updated this guide for v1.4.0rc3 of the iApp available on downloads.f5.com in the Release_Candidates directory. This version of the template contains no visible changes to the iApp presentation, and only one change: Corrected a failover issue for route table updates when IPv6 Self IP addresses are present. | 05-10-2018 |
| 1.9 | Added a note to the BIG-IP VE prerequisites stating you must be using a BIG-IP VE with 2 or more NICs. Using a single Network Interface deployment is not supported. | 06-21-2018 |
| 2.0 | Corrected the GitHub link for the Amazon CloudFormation template. | 12-14-2018 |
| 2.1 | Added a note to the prerequisites stating that this iApp does not support IPv6. | 01-07-2019 |
| 2.2 | Updated this guide for v1.4.0rc5 of the iApp available on downloads.f5.com. This version of the template contains the following changes: - Added logic to determine the version of Python installed on the BIG-IP - Removed EC2 tools dependencies by migrating to AWS CLI tools | 05-23-2019 |

F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 www.f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com

