BIG-IP® System: Clustering with Mirroring using ECMP

Version 12.1

Table of Contents

Introduction to All-Active Clustering Using ECMP

Overview: Configuring all-active clustering using ECMP

You can implement BIG-IP® high availability on a network by using the Equal Cost Multi-Path (ECMP) protocol. You do this by creating the same virtual IP address on each BIG-IP device in a Sync-Failover device group. Then the upstream router uses ECMP to determine if there are multiple, equal-cost paths to this virtual address. If there are, the router uses an algorithm to select a path to the external floating self IP address on any one of the BIG-IP devices.

With this configuration, an application is not pinned to a specific device; instead, all of the devices actively process the same application traffic. And you can add capacity at any time by adding a BIG-IP device to the device group, syncing the configuration to the new device, and then modifying the configuration on the upstream router.

This illustration shows an example of this configuration. Notice that each device in the device group has the same virtual address.

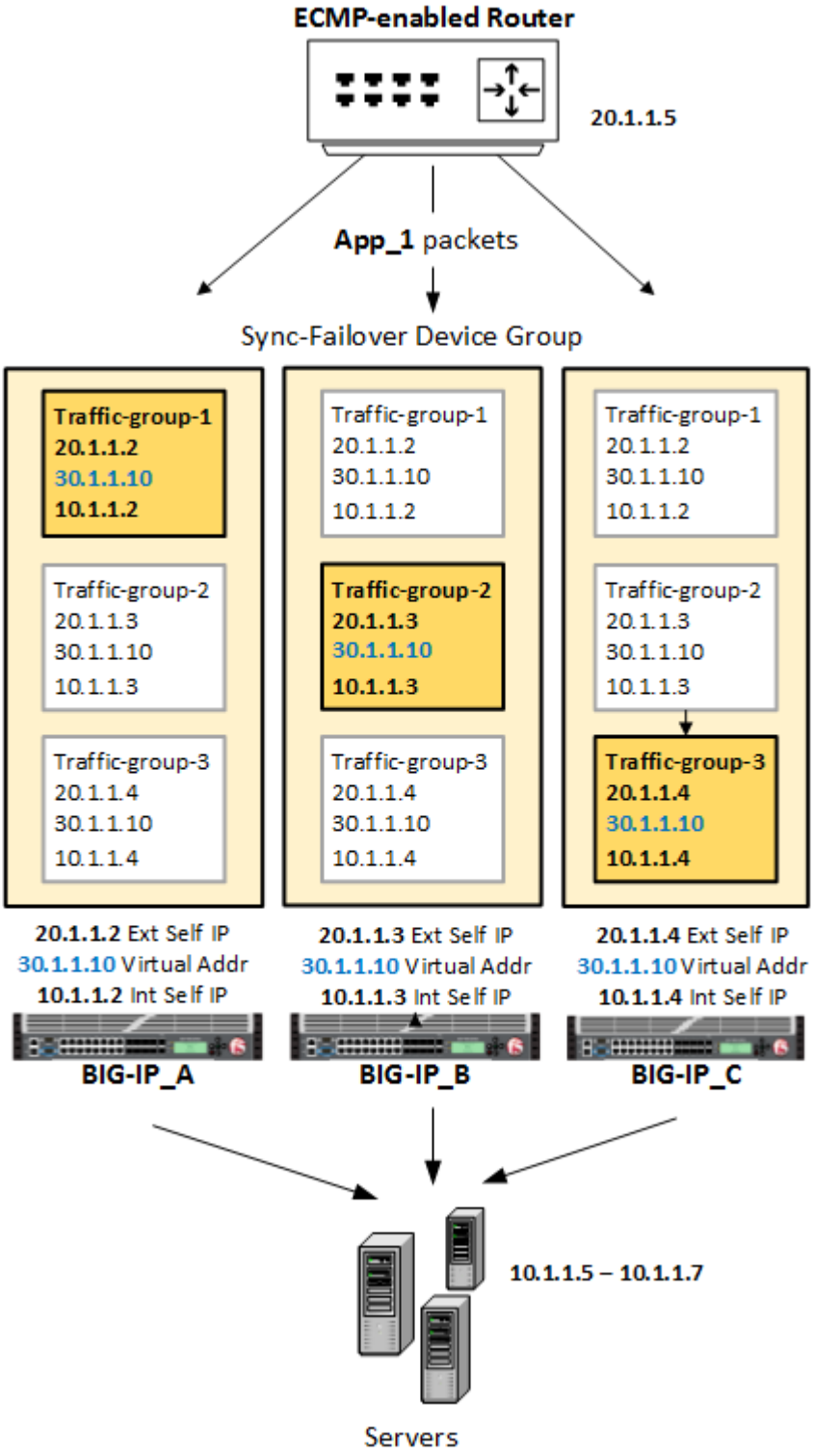

Figure 1: High-availability clustering using ECMP

The illustration shows that the floating virtual address has been configured to span all three BIG-IP devices. Each device also has an active traffic group containing a unique floating external self IP address and a unique floating internal self IP address. So the floating addresses for `BIGIP_A` are assigned to `traffic-group-1`, the addresses for `BIGIP_B` are assigned to `traffic-group-2`, and the `BIGIP_C` addresses are assigned to `traffic-group-3`.

On the upstream ECMP-enabled router, routes are configured to send packets for `App_1` to any of the three floating external self IP addresses. If an active traffic group fails over to another device, the packets targeting that traffic group's floating self IP address begin to target the same traffic group on the newly-active device. So for example, if `traffic-group-1` fails over to `BIGIP_B`, then any traffic destined for the external floating IP address `20.1.1.2` now targets the same address on `BIGIP_B`.

The floating internal self IP address within each traffic group ensures that on the return trip from a server, the packets go back through one of the BIG-IP devices. Using the SNAT Auto Map feature, a return packet will always target one of the floating internal self IP addresses in the device group.

Before you begin

Use this information to make sure that you have configured the prerequisites for this ECMP implementation.

Static route configuration

On the upstream ECMP-enabled router, make sure you configure a route to each floating external self IP address in the device group (one per device).

DNS servers (optional)

If you intend to use fully-qualified domain names (FQDNs) for either your server pool members or your NTP servers, you need to specify one or more DNS servers on each device.

Configuring the Basic BIG-IP Network

Overview: Configuring basic system settings

You configure the BIG-IP® system to handle traffic from an ECMP-enabled upstream router so that you get all-active BIG-IP clustering. Before you can do that, you need to complete some basic tasks for Traffic Management Operating System® (TMOS). These basic tasks include creating VLANs and self IP addresses, and then specifying your NTP servers. Other tasks involve creating a BIG-IP® device group and then syncing a BIG-IP configuration across all devices.

After finishing these tasks, you can configure LTM® to implement ECMP-based all-active clustering, with connection mirroring between BIG-IP devices.

Task List

Creating VLANs

VLANs represent a logical collection of hosts that can share network resources, regardless of their physical location on the network. You create a VLAN to associate physical interfaces with that VLAN. For this implementation, F5 Networks recommends that you create three VLANs on each BIG-IP® device: a VLAN for the external network, a VLAN for the internal network, and a VLAN for high availability communications. Examples of VLAN names are `External`, `Internal`, and `HA`.

Important: *You must perform this task locally on each BIG-IP device that is to be a member of the BIG-IP device group, and you must create the object in administrative partition* `Common`*.*

---

1. On the Main tab, click **Network** > **VLANs**.
   The VLAN List screen opens.
2. Click **Create**.
   The New VLAN screen opens.
3. In the **Name** field, type a unique name for the VLAN.
4. In the **Tag** field, type a numeric tag, between 1-4094, for the VLAN, or leave the field blank if you want the BIG-IP system to automatically assign a VLAN tag.

   The VLAN tag identifies the traffic from hosts in the associated VLAN.
5. If you want to use Q-in-Q (double) tagging, use the **Customer Tag** setting to perform the following two steps. If you do not see the **Customer Tag** setting, your hardware platform does not support Q-in-Q tagging and you can skip this step.
   a) From the **Customer Tag** list, select **Specify**.
   b) Type a numeric tag, from 1-4094, for the VLAN.

   The customer tag specifies the inner tag of any frame passing through the VLAN.
6. For the **Interfaces** setting:

a) From the **Interface** list, select an interface number.
b) From the **Tagging** list, select **Tagged** or **Untagged**.
Select **Tagged** when you want traffic for that interface to be tagged with a VLAN ID.
c) If you specified a numeric value for the **Customer Tag** setting and from the **Tagging** list you selected **Tagged**, then from the **Tag Mode** list, select a value.
d) Click **Add**.
e) Repeat these steps for each interface that you want to assign to the VLAN.

7. If you want the system to verify that the return route to an initial packet is the same VLAN from which the packet originated, select the **Source Check** check box.
8. In the **MTU** field, retain the default number of bytes (**1500**).
9. From the **Configuration** list, select **Advanced**.
10. If you want to base redundant-system failover on VLAN-related events, select the **Fail-safe** check box.
11. From the **Auto Last Hop** list, select a value.
12. From the **CMP Hash** list, select a value.
13. To enable the **DAG Round Robin** setting, select the check box.
14. Click **Finished**.
The screen refreshes, and displays the new VLAN in the list.

Creating static self IP addresses

Self IP addresses enable the BIG-IP® system, and other devices on the network, to route traffic through the associated VLAN. For this implementation, you perform this task on each BIG-IP device to create a unique static self IP address for each of the three VLANs (external, internal, and high availability). The BIG-IP systems within a device group use these self IP addresses to communicate with one another for config sync, failover, and mirroring. In this task, you replace any sample self IP names or IP addresses with the relevant self IP names or addresses for your network.

Important: *You must perform this task locally on each BIG-IP device that is to be a member of the BIG-IP device group, and you must create the self IP address in administrative partition* `Common`.

---

1. On the Main tab, click **Network** > **Self IPs**.
2. Click **Create**.
The New Self IP screen opens.
3. In the **Name** field, type a unique name for the static self IP address.
For example, for device `BIGIP_A`, this name could be `ext_static_self_bigipA` or `int_static_self_bigipA`.
4. In the **IP Address** field, type an IP address.
For example, in our sample configuration for device `BIGIP_A`, the static self IP address for VLAN `external` could be `20.1.1.6` .
5. In the **Netmask** field, type the network mask for the specified IP address.
For example, you can type `255.255.255.0`.
6. From the **VLAN/Tunnel** list, select the VLAN to associate with this self IP address.
   - On the internal network, select the internal or high availability VLAN that is associated with an internal interface or trunk.
   - On the external network, select the external VLAN that is associated with an external interface or trunk.
7. From the **Traffic Group** list, select **traffic-group-local-only (non-floating)**.
8. Click **Finished**.

The screen refreshes, and displays the new self IP address.

The BIG-IP system can send and receive traffic through the specified VLAN.

Specifying a list of NTP servers

If you use Dynamic Host Configuration Protocol (DHCP) to assign IP addresses to NTP servers, then before you perform this task, verify that you have configured a Domain Name System (DNS) server on the BIG-IP® system.

Network Time Protocol (NTP) synchronizes the clocks on a network of BIG-IP devices by means of a defined NTP server. This clock synchronization is required for successful operation of a BIG-IP device group. You can specify a list of the IP addresses of the defined NTP servers that you want the BIG-IP system to use when updating the time on BIG-IP systems on the network. Alternatively, you can specify a list of fully-qualified domain names.

Important: *You must perform this task locally on each BIG-IP device that is to be a member of the BIG-IP device group, and you must create the object in administrative partition* `Common`*.*

---

1. On the Main tab, click **System** > **Configuration** > **Device** > **NTP**.
   The NTP Device configuration screen opens.
2. Find the **Partition** list in the upper right corner of the BIG-IP Configuration utility screen, to the left of the **Log out** button.
3. From the **Partition** list, pick partition `Common`.
4. For the **Time Server List** setting, in the **Address** field, type the IP address of an NTP server that you want to add. Then click **Add**.

   Note: *If you are using Dynamic Host Configuration Protocol (DHCP) to assign IP addresses, then the BIG-IP system automatically populates the* ***Address*** *field with the fully-qualified domain name (FQDN) of the NTP server.*

   ---
5. Repeat the preceding step as needed.
6. Click **Update**.

Establishing device trust

Before you begin this task, verify that:

- Each BIG-IP® device that is to be part of the local trust domain has a device certificate installed on it.
- The local device is designated as a certificate signing authority.

You use this task to establish trust among devices on one or more network segments. Devices that trust each other make up the *local trust domain*. A device must be a member of the local trust domain before it can be part of a device group.

By default, the BIG-IP software includes a local trust domain with one member, which is the local device. You can choose any one of the BIG-IP devices slated for a device group and log into that device to add other devices to the local trust domain. For example, devices `Bigip_A`, `Bigip_B`, and `Bigip_C` each initially shows only itself as a member of the local trust domain. To configure the local trust domain to include all three devices, you can just log in to device `Bigip_A` and add devices `Bigip_B` and `Bigip_C` to the local trust domain; there is no need to repeat this process on devices `Bigip_B` and `Bigip_C`.

1. On the Main tab, click **Device Management** > **Device Trust**, and then either **Peer List** or **Subordinate List**.
2. Click **Add**.

3. Type a device IP address, administrator user name, and administrator password for the remote BIG-IP® device with which you want to establish trust. The IP address you specify depends on the type of BIG-IP device:
   - If the BIG-IP device is an appliance, type the management IP address for the device.
   - If the BIG-IP device is a VIPRION® device that is not licensed and provisioned for vCMP®, type the primary cluster management IP address for the cluster.
   - If the BIG-IP device is a VIPRION device that is licensed and provisioned for vCMP, type the cluster management IP address for the guest.
   - If the BIG-IP device is an Amazon Web Services EC2 device, type one of the Private IP addresses created for this EC2 instance.
4. Click **Retrieve Device Information**.
5. Verify that the certificate of the remote device is correct.
6. Verify that the management IP address and name of the remote device are correct.
7. Click **Finished**.

After you perform this task, the local device is now a member of the local trust domain.

Specifying config sync, failover, and mirroring addresses

Before configuring the config sync, failover, and mirroring addresses on a BIG-IP device, verify that all devices in the device group are running the same version of BIG-IP® system software.

You perform this task to specify IP addresses on the local device that other devices in the device group will use to:

- Synchronize their configuration objects to the local device.
- Assess the health status of the local device.
- Mirror connections to the local device.

Note: *You must perform this task locally on each device in the device group.*

---

1. Confirm that you are logged in to the device you want to configure.
2. On the Main tab, click **Device Management** > **Devices**.
   This displays a list of device objects discovered by the local device.
3. In the Name column, click the name of the device to which you are currently logged in.
4. From the Device Connectivity menu, choose ConfigSync.
5. For the **Local Address** setting, select the static self IP address for the internal VLAN.
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 VLAN `HA`. Then repeat the action, specifying the device's management IP address.
8. For the **Primary Local Mirror Address** setting, select the static self IP address for VLAN `internal`.
9. For the **Secondary Local Mirror Address** setting, select the static self IP address for VLAN `HA`.

   This setting is optional. The system uses the selected IP address in the event that the primary mirroring address becomes unavailable.
10. Click **Update**.

After you perform this task, the other devices in the device group can sync their configurations, fail over, and mirror their connections to the local device.

Creating a Sync-Failover device group

This task establishes failover capability between two or more BIG-IP® devices. If an active device in a Sync-Failover device group becomes unavailable, the configuration objects fail over to another member of the device group and traffic processing is unaffected. You perform this task on any one of the authority devices within the local trust domain.

1. On the Main tab, click **Device Management** > **Device Groups**.
2. On the Device Groups list screen, click **Create**.
   The New Device Group screen opens.
3. Type a name for the device group, select the device group type **Sync-Failover**, and type a description for the device group.
4. From the **Configuration** list, select **Advanced**.
5. In the Configuration area of the screen, select a host name from the **Available** list for each BIG-IP device that you want to include in the device group, including the local device. Use the Move button to move the host name to the **Includes** list.

   The **Available** list shows any devices that are members of the device's local trust domain but not currently members of a Sync-Failover device group. A device can be a member of one Sync-Failover group only.
6. For the **Network Failover** setting, select or clear the check box:
   - Select the check box if you want device group members to handle failover communications by way of network connectivity. This choice is required for active-active configurations.
   - Clear the check box if you want device group members to handle failover communications by way of serial cable (hard-wired) connectivity.

   For active-active configurations, you must select network failover, as opposed to serial-cable (hard-wired) connectivity.
7. For the **Automatic Sync** setting, select or clear the check box:

Action	Result
Select (Enable)	Select the check box when you want the BIG-IP system to automatically sync configuration data to device group members whenever a change occurs. When you enable this setting, the BIG-IP system automatically syncs, but does not save, the configuration change on each device (this is the default behavior). To save the updated configuration on each device, you can log in to each device and, at the `tmsh` prompt, type `save sys config`. Alternatively, you can change the default behavior so that the system automatically saves configuration changes on target devices after an automatic config sync. You make this change by logging in to one of the devices in the device group and, at the `tmsh` prompt, typing `modify cm device-group` *`name`* `save-on-auto-sync true`. ***Warning:*** *Enabling the* `save-on-auto-sync` *option can unexpectedly impact system performance when the BIG-IP system automatically saves a large configuration change to each device.*
Clear (Disable)	Clear the check box when you want to disable automatic sync. When this setting is disabled, you must manually initiate each config sync operation. F5 Networks® recommends that you perform a config sync whenever configuration data changes on one of the devices in the device group. After you perform a manual config sync, the BIG-IP system automatically saves the configuration change on each device group member.

8. For the **Full Sync** setting, specify whether the system synchronizes the entire configuration during synchronization operations:
   - Select the check box when you want all sync operations to be full syncs. In this case, every time a config sync operation occurs, the BIG-IP system synchronizes all configuration data associated with the device group. This setting has a performance impact and is not recommended for most customers.
   - Clear the check box when you want all sync operations to be incremental (the default setting). In this case, the BIG-IP system syncs only the changes that are more recent than those on the target device. When you select this option, the BIG-IP system compares the configuration data on each target device with the configuration data on the source device and then syncs the delta of each target-source pair.

   If you enable incremental synchronization, the BIG-IP system might occasionally perform a full sync for internal reasons. This is a rare occurrence and no user intervention is required.
9. In the **Maximum Incremental Sync Size (KB)** field, retain the default value of `1024`, or type a different value.

   This value specifies the total size of configuration changes that can reside in the incremental sync cache. If the total size of the configuration changes in the cache exceeds the specified value, the BIG-IP system performs a full sync whenever the next config sync operation occurs.
10. Click **Finished**.

You now have a Sync-Failover type of device group containing BIG-IP devices as members.

Syncing the BIG-IP configuration to the device group

Before you sync the configuration, verify that the devices that are targeted for config sync are members of a Sync-Failover device group.

This task synchronizes the latest BIG-IP® configuration data from the local device to the devices in the device group. This synchronization makes sure that devices in the device group work correctly.

Note: *You only need to do this task on one device in the device group.*

---

1. On the Main tab, click **Device Management** > **Overview**.
2. In the Device Groups area of the screen, from the Name column, select the name of the relevant device group.
   The screen expands to show a summary and details of the sync status of the selected device group, as well as a list of the individual devices within the device group.
3. In the Devices area of the screen, from the Sync Status column, select the device that shows a sync status of `Changes Pending`.
4. In the Sync Options area of the screen, select **Sync Device to Group**.
5. Click **Sync**.
   The BIG-IP system syncs the configuration data of the selected device in the Device area of the screen to the other members of the device group.

After you complete this task, the BIG-IP configuration data is synchronized to every device in the device group.

Completing the All-Active Configuration

Task summary

There are several tasks that you perform to implement a clustering configuration with an ECMP-enabled router.

Important: *To perform the tasks in this implementation, you must have the Administrator user role assigned to your user account for BIG-IP ® system.*

Task list

Creating a server pool

Before starting this task:

- Decide on the IP addresses or FQDNs for the servers that you want to include in your server pool.
- If your system is using DHCP, make sure your DNS servers are not configured for round robin DNS resolutions; instead, they should be configured to return all available IP addresses in a resolution.

Use this task to create a pool of servers with pool members. The pool identifies which servers you want the virtual server to send client requests to. As an option, you can identify the servers by their FQDNs instead of their IP addresses. In this way, the system automatically updates pool members whenever you make changes to their corresponding server IP addresses on your network.

1. On the Main tab, click **Local Traffic** > **Pools**.
   The Pool List screen opens.
2. Click **Create**.
   The New Pool screen opens.
3. In the **Name** field, type a unique name for the pool.
4. For the **Health Monitors** setting, from the **Available** list, select a monitor and move the monitor to the **Active** list.

   Note: *A pool containing nodes represented by FQDNs cannot be monitored by* `inband` *or* `sasp` *monitors.*

   ---

5. From the **Load Balancing Method** list, select how the system distributes traffic to members of this pool.

   The default is **Round Robin**.
6. For the **New Members** setting, add each server that you want to include in the pool:
   a) Select **New Node** or **New FQDN Node**.
   b) (Optional) In the **Node Name** field, type a name for the node.

c) If you chose **New Node**, then in the **Address** field, type the IP address of the server. If you chose **New FQDN Node**, then in the **FQDN** field, type the FQDN of the server.

If you want to use FQDNs instead of IP addresses, you should still type at least one IP address. Typing one IP address ensures that the system can find a pool member if a DNS server isn't available.

d) For the **Service Port** option, pick a service from the list.

e) If you are using FQDNs for the server names, then for **Auto Populate**, keep the default value of **Enabled**.

Note: *When you leave **Auto Populate** turned on, the system creates an ephemeral node for each IP address returned as an answer to a DNS query. Also, when a DNS answer shows that the IP address of an ephemeral node doesn't exist anymore, the system deletes the ephemeral node.*

---

f) Click **Add**.

g) Do this step again for each node.

7. Click **Finished**.

Creating a destination address and port for application traffic

Before you start this task, make sure you have specified primary and secondary mirroring IP addresses on each device in the device group.

Completing this task provides a destination for application traffic coming into the BIG-IP® system from an ECMP-enabled router on the network.

Note: *You only have to do this task on one device in the device group (in our example, `Bigip_A`). Later you will synchronize this configuration to the other devices in the device group.*

---

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Find the **Partition** list in the upper right corner of the BIG-IP Configuration utility screen, to the left of the **Log out** button.
3. From the **Partition** list, pick partition `Common`.
4. Click the **Create** button.
   The New Virtual Server screen opens.
5. In the **Name** field, type a unique name for the virtual server.
6. From the **Type** list, select **Standard**.
7. In the **Destination Address/Mask** field, type the IP address in CIDR format.

   The supported format is address/prefix, where the prefix length is in bits. For example, an IPv4 address/prefix is `10.0.0.1` or `10.0.0.0/24`, and an IPv6 address/prefix is `ffe1::0020/64` or `2001:ed8:77b5:2:10:10:100:42/64`. When you use an IPv4 address without specifying a prefix, the BIG-IP® system automatically uses a `/32` prefix.

   Note: *This address must be on a separate network available only through routing (instead of through a directly-connected network).*

   In our example, this address is `30.1.1.10`.
8. In the **Service Port** field, type a port number or select a service name from the **Service Port** list.
9. From the **Configuration** list, select **Advanced**.
10. From the **Source Address Translation** list, select **Auto Map**.
11. For the **Connection Mirroring** setting, select the check box.

Note: *This setting only appears when the BIG-IP device is a member of a device group.*

12. In the Resources area of the screen, from the **Default Pool** list, select the relevant pool name.
13. Configure any other settings that you need.
14. Click **Finished**.

The virtual server appears in the list of existing virtual servers on the Virtual Server List screen.

Enabling the virtual address to span all devices

For this ECMP setup, you will need to log in to the BIG-IP® device you created the virtual server and make sure that the associated virtual address is associated with the default traffic group (`traffic-group-1`). Then you will need to enable the **Spanning** option.

Note: *You only need to do this task on one device in the device group (in our example, `Bigip_A`). Later you will synchronize this configuration to the other devices in the device group.*

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen displays a list of existing virtual servers.
2. On the menu bar, click **Virtual Address List**.
   This displays the list of virtual addresses.
3. Click the name of the virtual address you want to view.
   This shows the properties of that virtual address.
4. Ensure that the **Traffic Group** list is set to `traffic-group-1`.

   Note: *`traffic-group-1` is the default floating traffic group on the system.*
5. Clear the **ARP** check box.
   This disables the Advanced Resolution Protocol (ARP).
6. Select the **Spanning** check box.
   This setting adds this floating virtual address to all floating traffic groups in the device group, ensuring that all devices in the device group can receive traffic from the ECMP-enabled upstream router.
7. Click **Update**.

Creating traffic groups for failover

On one of the devices in the device group, create the floating traffic groups you will need for your configuration, except for `traffic-group-1`, which is the default traffic group. Each new traffic group is empty after you create it.

1. On the Main tab, click **Device Management** > **Traffic Groups**.
2. On the Traffic Groups screen, click **Create**.
3. In the **Name** field, type a name for the new traffic group.
   An example of a traffic group name is `traffic-group-2`.
4. In the **Description** field, type a description for the new traffic group.
   For example, you can type `This traffic group contains the floating IP addresses that are on BIGIP_B.`
5. In the **MAC Masquerade Address** field, type a MAC masquerade address.

   For this setting, you should use an industry-standard method for creating a locally-administered MAC address. Each traffic group needs a MAC masquerade address to reduce the risk of dropped connections when failover happens.

6. From the **Failover Method** list, select **HA Order**.
7. Select the **Auto Failback** check box.
   This enables auto failback for the traffic group. When you combine auto failback with the **HA Order** setting you selected, each traffic group in the configuration goes active on a separate device, providing you with an all-active device group.
8. For the **Failover Order** setting, in the **Available** box, select the name of the device that you want this traffic group to be active on and then move it to the **Enabled** box. Repeat for each device that you want to be the next-active device if failover occurs.

   You can put only members of the device group on the ordered list. You can't put devices from the local trust domain on the list if they are not in the device group.

   In our sample device group, where we configured each traffic group to be active on a different device, the first device in `traffic-group-1`'s **Failover Order** list is `BIGIP_A`. Similarly, the first device in the `traffic-group-2` list is `BIGIP_B`, and the first device in the `traffic-group-3` list is `BIGIP_C`.
9. Click **Finished**.
10. Repeat this task for as many active traffic groups as you need for your configuration.

When you have finished configuring a traffic group (with auto-failback enabled), the traffic group goes active on the first device in the **Failover Order** list, even before any failover event happens. From then on, the traffic group always tries to be active on that device. If all of the devices in the ordered list are unavailable, and you have device group members that are not on the ordered list, the BIG-IP® system ignores the ordered list. Instead, it looks at the devices that are not on the list, and uses them to calculate a load-aware score for each of those devices, based on the local device's configured **HA Capacity** and the default **HA Load** value (`1`).

Creating floating self IP addresses

Each device in the BIG-IP® device group requires a *floating self IP address* to ensure that inbound or outbound traffic targeted to a BIG-IP device reaches its destination even when a device goes down and failover occurs. You can create the floating self IP addresses from just one of the devices in the device group (in our example, `Bigip_A`). Later, you will sync that device's configuration to the other devices in the device group. Using our sample configuration with three devices that each have an external and internal VLAN, this means you will create a total of six floating self IP addresses, each associated with a specific VLAN and a specific traffic group.

BIG-IP Device	VLAN `external`	VLAN `internal`	Traffic Group
Bigip_A	20.1.1.2	10.1.1.2	Traffic-group-1
Bigip_B	20.1.1.3	10.1.1.3	Traffic-group-2
Bigip_C	20.1.1.4	10.1.1.4	Traffic-group-3

1. On the Main tab, click **Network** > **Self IPs**.
2. Find the **Partition** list in the upper right corner of the BIG-IP Configuration utility screen, to the left of the **Log out** button.
3. From the **Partition** list, make sure that partition `Common` is selected.
4. Click **Create**.
   The New Self IP screen opens.
5. In the **Name** field, type a unique name for the floating self IP address.
   For example, for the floating external self IP address for device `Bigip_A`, this name could be `float_ext_self_bigipA`.
6. In the **IP Address** field, type an IP address.

For example, in our sample configuration for device `BIGIP_A`, the static self IP address for VLAN `external` could be `20.1.1.6` .

7. In the **Netmask** field, type the full network mask for the specified IP address.
8. From the **VLAN/Tunnel** list, select either **external** or **internal**.
9. Click **Add**.
10. From the **Traffic Group** list, select the name of a floating traffic group.
    For example, for IP address `20.1.1.2`, select `Traffic-group-1`. For address `20.1.1.3`, select `Traffic-group-2`, and so on.
11. Click **Finished**.
    The screen refreshes, and displays the new self IP address.
12. Repeat this task for each of the floating IP addresses that you want to be members of a traffic group.

Syncing the BIG-IP configuration to the device group

Before you sync the configuration, verify that the devices that are targeted for config sync are members of a Sync-Failover device group.

This task synchronizes the latest BIG-IP® configuration data from the local device to the devices in the device group. This synchronization makes sure that devices in the device group work correctly.

Note: *You only need to do this task on one device in the device group.*

---

1. On the Main tab, click **Device Management** > **Overview**.
2. In the Device Groups area of the screen, from the Name column, select the name of the relevant device group.
   The screen expands to show a summary and details of the sync status of the selected device group, as well as a list of the individual devices within the device group.
3. In the Devices area of the screen, from the Sync Status column, select the device that shows a sync status of `Changes Pending`.
4. In the Sync Options area of the screen, select **Sync Device to Group**.
5. Click **Sync**.
   The BIG-IP system syncs the configuration data of the selected device in the Device area of the screen to the other members of the device group.

After you complete this task, the BIG-IP configuration data is synchronized to every device in the device group.

Configuration Result

After following the instructions in this implementation, you should now have a BIG-IP® device group, where the same virtual server and virtual address reside on each device. Also, each traffic group is active on a different device.

With this configuration, when application traffic comes through the ECMP-enabled router, the router can use an algorithm to choose the best equal-cost path to send the same application's traffic to any one of the BIG-IP devices in the device group. If any of the BIG-IP devices becomes unavailable, the ECMP-enabled router is able to send that traffic to another device in the device group. All devices in the device group use the default load balancing pool to service application traffic.

Configuration result

After following the instructions in this implementation, you should now have a BIG-IP® device group, where the same virtual server and virtual address reside on each device. Also, each traffic group is active on a different device.

With this configuration, when application traffic comes through the ECMP-enabled router, the router can use an algorithm to choose the best equal-cost path to send the same application's traffic to any one of the BIG-IP devices in the device group. If any of the BIG-IP devices becomes unavailable, the ECMP-enabled router is able to send that traffic to another device in the device group. All devices in the device group use the default load balancing pool to service application traffic.

Legal Notices

Legal notices

Publication Date

This document was published on May 9, 2016.

Publication Number

MAN-0616-00

Copyright

Trademarks

For a current list of F5 trademarks and service marks, see *http://www.f5.com/about/guidelines-policies/trademarks/*.

All other product and company names herein may be trademarks of their respective owners.

Patents

This product may be protected by one or more patents indicated at: *https://f5.com/about-us/policies/patents*

Export Regulation Notice

This product may include cryptographic software. Under the Export Administration Act, the United States government may consider it a criminal offense to export this product from the United States.

RF Interference Warning

This is a Class A product. In a domestic environment this product may cause radio interference, in which case the user may be required to take adequate measures.

FCC Compliance

This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This unit generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user, at his own expense, will be required to take whatever measures may be required to correct the interference.

Any modifications to this device, unless expressly approved by the manufacturer, can void the user's authority to operate this equipment under part 15 of the FCC rules.

Canadian Regulatory Compliance

This Class A digital apparatus complies with Canadian ICES-003.

Standards Compliance

This product conforms to the IEC, European Union, ANSI/UL and Canadian CSA standards applicable to Information Technology products at the time of manufacture.

Index