VIPRION® Systems: Configuration

Version 13.0

Table of Contents

VIPRION System Overview

What is a VIPRION system?

The VIPRION® system is a complete traffic management solution that offers high performance, reliability, scalability, and ease of management. Based on chassis and blade technology, this system is designed to meet the needs of large, enterprise networking environments that normally require multiple BIG-IP® systems to process large volumes of application traffic.

The VIPRION system includes multiple blades that work together as a powerful *cluster* to process application traffic. When traffic comes into a single virtual server, the system distributes that traffic over multiple blades using the full multi-processing capacity of each blade. This ensures that other blades can complete the processing of the request if one unexpectedly becomes unavailable.

This illustration shows a typical VIPRION system with a four-slot cluster processing traffic destined for virtual server `vs_http`. In this example, the virtual server resides on all blades in the cluster, due to a process known as *cluster synchronization*. The primary blade receives the client traffic and then uses the power of all blades in the cluster to process the traffic before sending the traffic to the appropriate server.

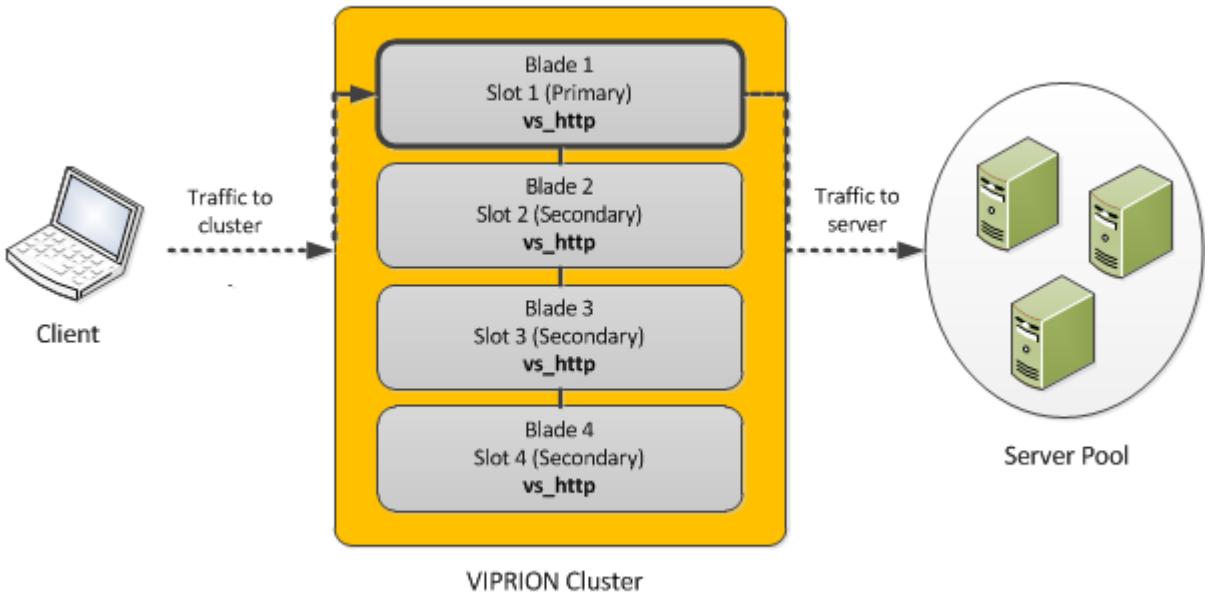

Figure 1: Example of a basic VIPRION system

About the VIPRION cluster

The VIPRION® system includes SuperVIP® cluster technology, the core feature that coordinates all of the blades into a single high-performance system. A *cluster* is a group of active slots in the VIPRION system chassis. The size of the cluster depends on the number of running blades installed in the chassis. Cluster

technology provides the processing power of multiple blades, but you manage the entire cluster as a single system. When you install a blade in a slot and power on the blade, the slot automatically becomes a member of the cluster.

Each slot in the cluster represents a cluster member, and the blades in the slots of a cluster work together to process application traffic. Moreover, the blades can be configured to mirror each other's connections so that if a blade is taken out of service or becomes unavailable for some reason, any in-process connections remain intact.

Note: *When two chassis are in a redundant system configuration, the VIPRION system mirrors the connections and session persistence records that the blades in a cluster are processing to the cluster in the other chassis. You can configure inter-cluster mirroring, for a redundant system configuration only, and only when the identical number of blades are present in the identical slot numbers in each of the two clusters of the redundant system configuration.*

About the cluster IP address

One of the tasks you performed as part of the hardware installation was to assign a unique cluster IP address to the primary slot in the cluster. This *cluster IP address* is a floating management IP address used to access the blade in the primary slot to manage the system. If the blade in the primary slot becomes unavailable for any reason, the primary designation moves to a different slot, and the cluster IP address floats to that slot.

About cluster synchronization

The VIPRION® system automatically performs *cluster synchronization*, an internal process that causes the primary blade to automatically propagate the BIG-IP ®software configuration to all secondary blades, even when a new blade is introduced into the cluster. Cluster synchronization allows all blades in the cluster to work together to process incoming traffic, and ensures that you can always access the cluster using the cluster IP address, even when the blade in the primary slot changes.

About chassis and blade models

The number of slots in a chassis varies depending on the chassis model. For example, while some chassis models contain two or four slots, the VIPRION® C4800 Series contains eight slots.

Each chassis model requires a specific blade type. For example, the VIPRION C4800 chassis uses VIPRION B4300 Series blades. For specific information on blade types compatible with your chassis, consult the platform guide for your chassis series.

About Virtualized Clustered Multi-Processing

If you need multi-tenancy, you can optionally provision the VIPRION® system for virtual Clustered Multiprocessing (vCMP®). Provisioning vCMP creates a hypervisor and allows you to create guests on the system for multi-tenant processing.

This illustration shows a basic vCMP system with a host and four guests. Note that each guest has a different set of modules provisioned, depending on the guest's particular traffic requirements.

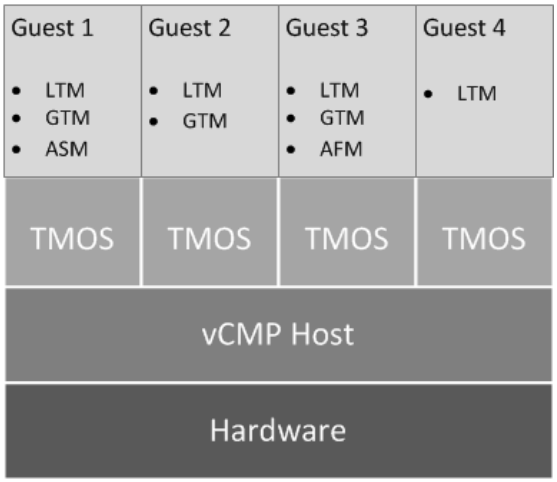

Figure 2: Example of a four-guest vCMP system on a VIPRION chassis

For more information, see the vCMP product documentation at F5 Networks® knowledge web site `http://support.f5.com`.

Summary of cluster-related terms

There are several cluster-related terms that are helpful to understand.

Term	Definition
cluster	The group of active slots in the chassis. The blades in the cluster work together as one powerful system to process application traffic. Also known as a *SuperVIP® cluster*.
cluster member	An enabled physical slot (or a virtual slot) that contains an active blade.
cluster IP address	The floating management IP address of the slot designated as the primary slot. You normally assign the cluster IP address during VIPRION chassis installation.
primary slot	The slot containing the blade that initially accepts application traffic. The floating cluster IP address is assigned to the primary slot. If the blade in the primary slot becomes unavailable, the cluster IP address automatically floats to another cluster member and the slot of the new cluster member becomes the primary slot.
primary blade	The blade residing in the primary slot.
secondary slot	Any slot that is not the primary slot and therefore does not have the floating cluster IP address assigned to it.
secondary blade	Any blade residing in a secondary slot.
cluster member IP address	The static management IP address assigned to a cluster member.

Term	Definition
cluster synchronization	An ongoing, internal process by which the primary blade automatically propagates the BIG-IP® system configuration to all secondary blades when powered-on. Cluster synchronization allows all blades in the cluster to work together to process network traffic.

Initial VIPRION Setup

Overview: Initial VIPRION system setup

After hardware installation is completed, you are ready to create a basic BIG-IP® software configuration.

Important: *Prior to configuring the BIG-IP software, verify that you have cabled the management interfaces of all slots to all of the blades, to minimize any interruption in service if a blade becomes unavailable.*

The first step in configuring the BIG-IP software is to run the Setup utility to perform tasks such as activating the BIG-IP system license and provisioning BIG-IP modules. You then set up a base BIG-IP system network consisting of trunks, VLANs, and self IP addresses, as well as a management IP address for each blade in the VIPRION® cluster. You also define your Domain Name System (DNS) servers and your NTP servers.

This illustration shows a basic VLAN and trunk configuration for a standalone VIPRION system. In the illustration, the VIPRION chassis is configured with a cluster containing two active blades. Note that each VLAN consists of two interfaces, one per slot. After setting up this basic configuration, you can adjust the configuration later as needed.

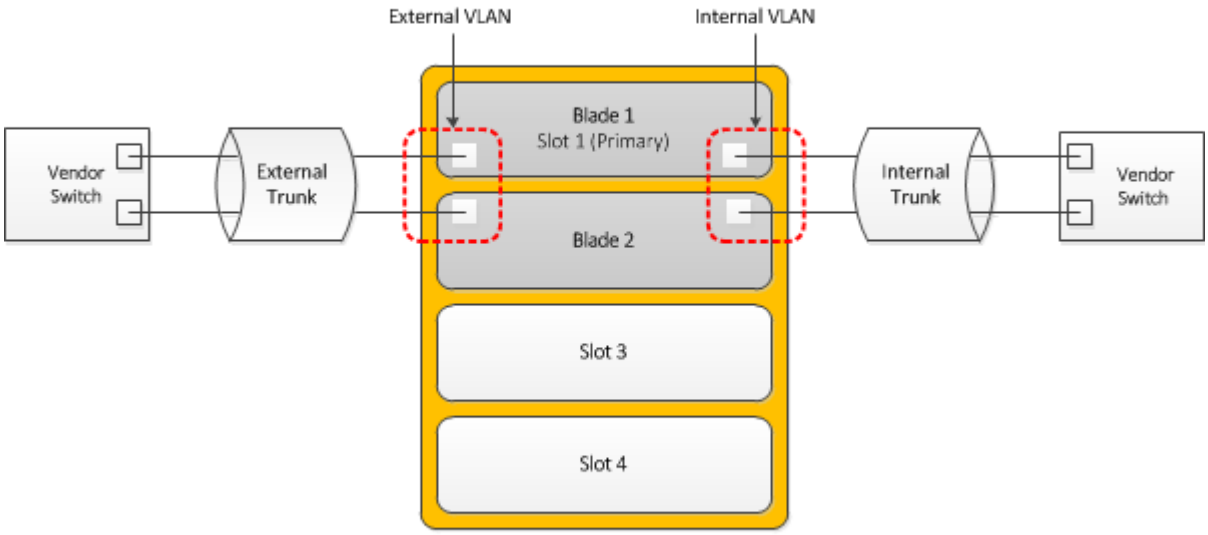

Figure 3: Basic VLAN and trunk configuration on a VIPRION system

About vCMP application volumes

During VIPRION® setup, before you provision the system, you must decide:

- If you're going to provision the system to run the Virtual Clustered Multiprocessing (vCMP®) feature
- Whether you want vCMP to consume the standard amount of disk space for vCMP on each blade

The total disk space that the system normally allocates to vCMP is determined by the size of each application volume (one per blade) that the system creates during vCMP provisioning.

By default, the BIG-IP system allocates all but 30 gigabytes of reserve disk space per blade to vCMP. *Reserve disk space* is the amount of disk space that the system reserves for other uses during provisioning, such as for installing other versions of the BIG-IP® system in the future. The reserved disk space also protects against any potential resizing of the file system.

Important: *You can change the reserve disk space for a vCMP application volume if you think that 30 gigabytes won't be sufficient, but you must do this before you provision the system for vCMP.*

Modifying disk space for a vCMP application volume

Use this procedure to increase the amount of reserve disk space on a vCMP application volume. Increasing reserve disk space allows you to install additional versions of the BIG-IP system, and protects against any potential resizing of the file system. The default reserve disk space is 30 gigabytes.

Important: *You must do this task before you provision the system for vCMP.*

Note: *When increasing the reserve disk space for additional BIG-IP installations, we recommend that you reserve 8 gigabytes per installation.*

1. In the URL field, type the management IP address that you previously assigned to the system.

   `https://<ip_address>`

   The browser displays the login screen for the BIG-IP Configuration utility.
2. On the Main tab, click **System** > **Disk Management**.
   The display shows the logical disks and application volumes from the perspective of the vCMP host.
3. Click the logical disk for which you want to reserve disk space.
   An example of a logical disk is `HD1`.
4. On the menu bar, click **Image List** if displayed.

   The screen displays a list of the installed images on the system.
5. If a list of images appears, locate the relevant image, and in the Disk column, click the logical disk name.
6. In the **Reserved (MB)** field, increase the amount of disk space that you want to reserve for the logical disk.

   The more space you reserve, the less disk space there is available for the vCMP application volume.
7. Click **Update**.

Running the Setup utility

Before you begin, confirm that you have done the following:

- Cabled the management interfaces of all slots in the chassis to all blades.
- Obtained the BIG-IP® base registration key.
- If you intend to provision the system for vCMP®, verified that the vCMP application volume has adequate reserve disk space for your system needs; you cannot adjust the reserve disk space after provisioning the system for vCMP.

Use this procedure to open the Setup utility and perform some basic, system- and network-level setup tasks. These tasks are a required part of initially configuring the BIG-IP software on the VIPRION® platform.

1. From a workstation attached to the management network, type the management IP address, using the following URL syntax: `https://<management_IP_address>`
2. At the login prompt, type the default user name `admin`, and password `admin`, and click **Log in**.
   The Setup utility screen opens.
3. Click **Next**.
   The General Properties screen opens.
4. Click **Activate**.
   The License screen opens.
5. In the **Base Registration Key** field, paste the registration key.

   You received your registration key when you purchased the BIG-IP device or module.
6. Click **Next**.
7. Provision selected BIG-IP modules (or the vCMP feature) to **Nominal**.

   If you are provisioning the vCMP feature, the BIG-IP® system allocates disk space for vCMP. By default, reserves 30 gigabytes of the total disk space for other uses, such as for installing additional versions of the BIG-IP system in the future. Before you provision vCMP, make sure the default reserved disk space is adequate for your needs; you cannot adjust the reserve disk space after provisioning the system for vCMP.

   Important: *When increasing the reserve disk space for additional BIG-IP installations, the recommended amount of space to reserve is 8 gigabytes per installation.*

   ---
8. Click **Next**.
   The device certificate is displayed.
9. Click **Next**.
   The General Properties and User Administration screen opens.
10. For the management IP address, specify the primary cluster IP address if the address was not assigned during hardware installation.
11. Specify a management IP address for each slot in the chassis if the addresses were not assigned during hardware installation.

    F5 Networks recommends that you specify an address for every slot in the chassis, regardless of the number of active cluster members. Doing so provides an IP address for any additional blades that you might install in the future.
12. In the **Host Name** field, type the host name of this BIG-IP system.
    For example, `www.siterequest.com`.
    The BIG-IP system prompts you to log in again.
13. Log in to the BIG-IP system.
    The BIG-IP system license is now activated, and selected BIG-IP modules are provisioned. The standard network configuration screen within the Setup utility is displayed.
14. Click **Finished**.

About trunk configuration

For VIPRION® platforms, F5 Networks® strongly recommends that you create a trunk for each of the BIG-IP® system internal and external networks, and that each trunk contains interfaces from all slots in the cluster.

For example, a trunk for the external network should contain the external interfaces of all blades in the cluster. Configuring a trunk in this way prevents interruption in service if a blade in the cluster becomes unavailable and minimizes use of the high-speed backplane when processing traffic.

Also, you should connect the links in a trunk to a vendor switch on the relevant network.

Important: *When processing egress packets, including those of vCMP® guests, the BIG-IP system uses trunk member interfaces on local blades whenever possible. This behavior ensures efficient use of the backplane, thereby conserving backplane bandwidth for processing ingress packets.*

Creating a trunk

You create a trunk on the BIG-IP® system so that the system can then aggregate the links to enhance bandwidth and ensure link availability.

1. On the Main tab, click **Network** > **Trunks**.
   The Trunk List screen opens.
2. Click **Create**.
3. Name the trunk.
4. For the **Interfaces** setting, in the **Available** field, select an interface, and using the Move button, move the interface to the **Members** field. Repeat this action for each interface that you want to include in the trunk.

   Trunk members must be untagged interfaces and cannot belong to another trunk. Therefore, only untagged interfaces that do not belong to another trunk appear in the **Available** list.
5. Select the **LACP** check box.
6. Click **Finished**.

After you create a trunk, the BIG-IP system aggregates the links to enhance bandwidth and prevent interruption in service.

About VLAN configuration

For the most basic BIG-IP® system configuration with redundancy enabled, you typically create multiple VLANs. That is, you create a VLAN for each of the internal and external networks, as well as a VLAN for high availability communications. You then associate each VLAN with the relevant interfaces of all cluster members on that network.

For example, for a system with a two-slot cluster, you might associate the external VLAN with interfaces `2.1/1` and `2.1/2`, where `2.1/1` is on slot 1 and `2.1/2` is on slot 2.

If your hardware platform supports ePVA, you have the additional option of configuring double tagging (also known as Q-in-Q tagging) for a VLAN.

Creating a VLAN

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 traffic destined for a specific address space. For the most basic BIG-IP® system configuration with redundancy enabled, you typically create multiple VLANs. That is, you create a VLAN for each of the internal and external networks, as well as a VLAN for high availability communications. If your hardware platform supports ePVA, you have the additional option of configuring double tagging (also known as Q-in-Q tagging) for a VLAN.

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. From the **Customer Tag** list:
   a) Retain the default value of **None** or select **Specify**.
   b) If you chose **Specify** in the previous step, type a numeric tag, between 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 or trunk name.
   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 or trunk 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. Configure the sFlow settings or retain the default values.
11. Click **Finished**.
    The screen refreshes, and displays the new VLAN in the list.

After you create the VLAN, you can assign the VLAN to a self IP address.

After creating the VLAN, ensure that you repeat this task to create as many VLANs as needed.

About self IP address configuration

When you do not intend to provision the vCMP® feature, you typically create self IP addresses when you initially configure the BIG-IP® system on the VIPRION® platform.

If you plan to provision vCMP, you do not need to create self IP addresses during initial BIG-IP configuration. Instead, the host administrator creates VLANs for use by guests, and the guest administrators create self IP addresses to associate with those VLANs.

Creating a self IP address

Before you create a self IP address, ensure that you have created a VLAN that you can associate with the self IP address.

A self IP address that you create within a guest enables the guest to route application traffic through the associated VLAN or VLAN group. On vCMP systems, a guest administrator creates self IP addresses and associates them with VLANs created on the host that a host administrator published to the guest during initial guest creation.

1. On the Main tab of the BIG-IP Configuration utility, click **Network** > **Self IPs**.

2. Click **Create**.
   The New Self IP screen opens.
3. In the **Name** field, type a unique name for the self IP address.
4. In the **IP Address** field, type an IPv4 or IPv6 address.

   This IP address should represent the address space of the VLAN that you specify with the **VLAN/ Tunnel** setting.
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 **Port Lockdown** list, select **Allow Default**.
8. From the **Traffic Group** list, select **traffic-group-local-only (non-floating)**.
9. From the **Service Policy** list, retain the default value of **None**, or select a policy to associate with the self IP address.

   A service policy contains a timer policy, which defines custom timeouts for matched traffic types.
10. Click **Finished**.
    The screen refreshes, and displays the new self IP address.

After creating a self IP address, a vCMP guest can send and receive traffic through the specified VLAN.

Specifying DNS servers

Use this procedure to specify the IP addresses of DNS servers on your network.

1. On the Main tab, click **System** > **Configuration** > **Device** > **DNS**
2. For each setting, in the **Address** field, type one or more IP addresses and click **Add**.
3. Click **Update**.

Defining an NTP server

Network Time Protocol (NTP) synchronizes the clocks on a network by means of a defined NTP server. You can specify a list of IP addresses of the servers that you want the BIG-IP® system to use when updating the time on network systems.

1. On the Main tab, click **System** > **Configuration** > **Device** > **NTP**.
   The NTP Device configuration screen opens.
2. For the **Time Server List** setting, in the **Address** field, type the IP address of the NTP server that you want to add. Then click **Add**.

   Note: *If you did not disable DHCP before the first boot of the BIG-IP system, and if the DHCP server provides the information about your NTP server, then this field is automatically populated.*
3. Click **Update**.

Configuration results

After you perform initial BIG-IP ®configuration, you have a standalone VIPRION® system that contains these configuration items:

- An active license
- One or more BIG-IP modules, or the vCMP® feature, provisioned
- A host name, management IP address, and management gateway defined
- Passwords for the `root` and `admin` passwords
- A valid device certificate
- A primary cluster IP address and a management IP address per slot
- Trunks for the external and internal networks
- VLANs for the external and internal networks that include all relevant interfaces for active blades
- A VLAN for high availability if redundancy is enabled
- Self IP addresses for the external and internal VLANs (if vCMP is not enabled)

Important: *When you ran the Setup utility, you enabled the local system for redundancy, but you did not actually configure redundancy with a VIPRION peer (by establishing device trust, creating a device group, and so on). You can configure redundancy with a peer system after you have repeated the initial VIPRION setup tasks on the peer system. For more information, see the F5 Networks® Knowledge web site at* `http://support.f5.com`.

Next steps

After the VIPRION® is configured with a base BIG-IP® network, the next step depends on whether you intend to use the vCMP® feature:

- If you do not intend to use vCMP, you can proceed with configuring any BIG-IP modules that you have provisioned. For example, for BIG-IP® Local Traffic Manager™, you can start by configuring various traffic profiles, creating a server pool, and creating a virtual server. You can then configure redundancy with a peer system and sync the BIG-IP configuration to the peer.
- If you intend to use vCMP, you must provision the system for vCMP only, create vCMP guests, and then configure redundancy with a peer system.

For more information on configuring the vCMP feature, BIG-IP product modules, and redundancy, access the F5 Networks® Knowledge web site at `http://support.f5.com`..

Managing a VIPRION cluster

About cluster management

When you initially configure the BIG-IP® software on a VIPRION® system, all installed blades automatically become members of the VIPRION cluster. A VIPRION *cluster* is the group of active slots in the chassis. The blades in the cluster work together as one powerful system to process network traffic. You can view the properties of the cluster and its members, enable and disable cluster members, and change cluster member IP addresses.

Viewing cluster properties

You can use the BIG-IP® Configuration utility to view the properties for the cluster.

1. Use a browser to log in to the VIPRION® chassis, using the primary cluster management IP address. If you provisioned the system for vCMP®, this step logs you in to the vCMP host.
2. On the Main tab, click **System** > **Clusters**.
   The Cluster screen opens, showing the properties of the cluster, and listing the cluster members.

Cluster properties

The Cluster screen displays the properties of the cluster.

Property	Description
Name	Displays the name of the cluster.
Cluster IP Address	Specifies the IP address assigned to the cluster. Click this IP address to change it.
Network Mask	Displays the network mask for the cluster IP address.
Primary Member	Displays the number of the slot that holds the primary blade in the cluster.
Software Version	Displays the version number of the BIG-IP® software that is running on the cluster.
Software Build	Displays the build number of the BIG-IP software that is running on the cluster.
Hotfix Build	Displays the build number of any BIG-IP software hotfix that is running on the cluster.
Chassis 400-level BOM	Displays the bill-of-materials (BOM) number for the chassis.
Status	Displays an icon and descriptive text that indicates whether there are sufficient available members of the cluster.

Viewing cluster member properties

You can use the BIG-IP® Configuration utility to view the properties for cluster members.

1. Use a browser to log in to the VIPRION® chassis, using the primary cluster management IP address. If you provisioned the system for vCMP®, this step logs you in to the vCMP host.
2. On the Main tab, click **System** > **Clusters**.
   The Cluster screen opens, showing the properties of the cluster, and listing the cluster members.
3. To display the properties for one cluster member, click the slot number of that member.
   The Cluster Member properties screen opens, showing the properties of that member.

Cluster member properties

In addition to displaying the properties of the cluster, the Cluster screen also lists information about members of the cluster. The table lists the information associated with each cluster member.

Property	Description
Status	The Status column indicates whether the cluster member is available or unavailable.
Slot	The Slot column indicates the number of the slot. Click this number to display the properties of that cluster member.
Blade serial number	The Blade Serial Number column displays the serial number for the blade currently in that slot.
Enabled	The Enabled column indicates whether that cluster member is currently enabled.
Primary	The Primary column indicates whether that cluster member is currently the primary slot.
HA State	The HA State column indicates whether the cluster member is used in a redundant system configuration for high availability.

Enabling and disabling cluster members

To gracefully drain the connections from a cluster member before you take that blade out of service, you can mark that cluster member disabled. Before you can return that member to service, you need to enable it.

1. Use a browser and the cluster management IP address to log in to the system and access the BIG-IP® Configuration utility.
2. On the Main tab, click **System** > **Clusters**.
   The Cluster screen opens, showing the properties of the cluster, and listing the cluster members.
3. Locate the cluster member you want to enable or disable, and select the box to the left of the Status icon.
4. Click **Enable** or **Disable/Yield**.

Changing a cluster IP address

You can use the BIG-IP® Configuration utility to view or change the either the floating management IP address for the cluster or an individual management IP address for a cluster member.

1. Use a browser and the cluster management IP address to log in to the system and access the BIG-IP® Configuration utility.
2. On the Main tab, click **System** > **Clusters**.
   The Cluster screen opens, showing the properties of the cluster, and listing the cluster members.
3. On the menu bar, click **Management IP Address**.
   The Management IP Address screen opens.
4. Locate the management IP address for the cluster or a cluster member IP address that you would like to change, and type the new IP address.
5. Click **Update**.

The specific IP address that you edited is changed. You can now use the new address to access the cluster.

Cluster-related IP addresses

This table describes the cluster-related addresses that you can modify.

Setting Type	Setting	Description
Cluster IP address	**IP Address**	Specifies the floating management IP address that you want to assign to the cluster. This IP address is used to access the Configuration utility, as well as to function as a cluster identifier for the peer cluster in a device service clustering configuration.
Cluster IP address	**Network Mask**	Specifies the network mask for the cluster IP address.
Cluster IP address	**Management Route**	Specifies the gateway for the cluster IP address. Typically, this is the default route.
Cluster Member IP Address	**Slot 1 IP Address**	Specifies the management IP address associated with slot 1 of the cluster. You can also set this value to **None**.
Cluster Member IP Address	**Slot 2 IP Address**	Specifies the management IP address associated with slot 2 of the cluster. You can also set this value to **None**.
Cluster Member IP Address	**Slot 3 IP Address**	Specifies the management IP address associated with slot 3 of the cluster. You can also set this value to **None**.
Cluster Member IP Address	**Slot 4 IP Address**	Specifies the management IP address associated with slot 4 of the cluster. You can also set this value to **None**.

High Availability Configuration

About DSC configuration on a VIPRION system

The way you configure device service clustering (DSC®) (also known as high availability) on a VIPRION® system varies depending on whether the system is provisioned to run the vCMP® feature.

Important: *When configuring high availability, always configure network, as opposed to serial, failover. Serial failover is not supported for VIPRION® systems.*

DSC configuration for non-vCMP VIPRION systems

For a Sync-Failover device group that consists of VIPRION® systems that are not licensed and provisioned for vCMP®, each VIPRION cluster constitutes an individual device group member. The following table describes the IP addresses that you must specify when configuring high availability.

Table 1: Required IP addresses for DSC configuration on a non-vCMP system

Feature	IP addresses required
Device trust	The primary floating management IP address for the VIPRION cluster.
ConfigSync	The unicast non-floating self IP address assigned to VLAN `internal`.
Failover	• Recommended: The unicast non-floating self IP address that you assigned to an internal VLAN (preferably VLAN `HA`), as well as a multicast address. • Alternative: All unicast management IP addresses that correspond to the slots in the VIPRION cluster.
Connection mirroring	For the primary address, the non-floating self IP address that you assigned to VLAN `HA`. The secondary address is not required, but you can specify any non-floating self IP address for an internal VLAN. ***Important:*** *Connection mirroring requires that both devices have identical hardware platforms (chassis and blades). If you plan to enable connection mirroring between two VIPRION chassis, each chassis within the Sync-Failover device group must contain the same number of blades in the same slot numbers. For more information, see the section Configuring connection mirroring between VIPRION clusters.*

Important: *When configuring high availability, always configure network, as opposed to serial, failover. Serial failover is not supported for VIPRION® systems.*

DSC configuration for vCMP systems

On a vCMP® system, the devices in a device group are virtual devices, known as *vCMP guests*. You configure device trust, config sync, failover, and mirroring to occur between equivalent vCMP guests in separate chassis.

For example, if you have a pair of VIPRION® systems running vCMP, and each system has three vCMP guests, you can create a separate device group for each pair of equivalent guests. This table shows an example.

Table 2: Sample device groups for two VIPRION systems with vCMP

Device groups for vCMP	Device group members
`Device-Group-A`	• `Guest1` on chassis1 • `Guest1` on chassis2
`Device-Group-B`	• `Guest2` on chassis1 • `Guest2` on chassis2
`Device-Group-C`	• `Guest3` on chassis1 • `Guest3` on chassis2

By isolating guests into separate device groups, you ensure that each guest synchronizes and fails over to its equivalent guest. The next table describes the IP addresses that you must specify when configuring high availability.

Table 3: Required IP addresses for DSC configuration on a VIPRION system with vCMP

Feature	IP addresses required
Device trust	The cluster management IP address of the guest.
ConfigSync	The non-floating self IP address on the guest that is associated with VLAN `internal` on the host.
Failover	• Recommended: The unicast non-floating self IP address on the guest that is associated with an internal VLAN on the host (preferably VLAN `HA`), as well as a multicast address. • Alternative: The unicast management IP addresses for all slots configured for the guest.
Connection mirroring	For the primary address, the non-floating self IP address on the guest that is associated with VLAN `internal` on the host. The secondary address is not required, but you can specify any non-floating self IP address on the guest that is associated with an internal VLAN on the host. ***Important:*** *Connection mirroring requires that both devices have identical hardware platforms (chassis and blades). If you plan to enable connection mirroring between two guests, each guest must reside on a separate chassis, be assigned to the same number of blades in the same slot numbers, and have the same number of cores allocated per slot. For more information, see the section Configuring connection mirroring between VIPRION clusters.*

Important: *When configuring high availability, always configure network, as opposed to serial, failover. Serial failover is not supported for VIPRION® systems.*

About DSC configuration for systems with APM

When you configure a VIPRION® system (or a VIPRION system provisioned for vCMP®) to be a member of a Sync-Failover device group, you can specify the minimum number of cluster members (physical or virtual) that must be available to prevent failover. If the number of available cluster members falls below the specified value, the chassis or vCMP guest fails over to another device group member.

When one of the BIG-IP® modules provisioned on your VIPRION® system or guest is Application Policy Manager ®(APM®), you have a special consideration. The BIG-IP system automatically mirrors all APM session data to the designated next-active device instead of to an active member of the same VIPRION or vCMP cluster. As a result, unexpected behavior might occur if one or more cluster members becomes unavailable.

To prevent unexpected behavior, you should always configure the chassis or guest so that the minimum number of available cluster members required to prevent failover equals the total number of defined cluster members. For example, if the cluster is configured to contain a total of four cluster members, you should specify the **Minimum Up Members** value to be `4`, signifying that if fewer than all four cluster members are available, failover should occur. In this way, if even one cluster member becomes unavailable, the system or guest will fail over to the next-active mirrored peer device, with full cluster member availability.

About connection mirroring for VIPRION systems

For VIPRION® systems, each device in a Sync-Failover device group can be either a physical cluster of slots within a chassis, or a virtual cluster for a vCMP® guest. In either case, you can configure a device to mirror an active traffic group's connections to its next-active device.

Important: *For mirroring to work, both the active device and its next-active device must have identical chassis platform and blade models.*

You enable connection mirroring on the relevant virtual server, and then you configure each VIPRION cluster or vCMP guest to mirror connections by choosing one of these options:

Within a cluster

You can configure the BIG-IP system to mirror connections between blades within a single VIPRION cluster on the same chassis. This option is not available on VIPRION systems provisioned to run vCMP.

Note: *With this option, the BIG-IP system mirrors Fast L4 connections only.*

Between clusters (recommended)

You can configure the BIG-IP system to mirror connections between two chassis or between two vCMP guests that reside in separate chassis. When you choose this option, the BIG-IP system mirrors a traffic group's connections to the traffic group's next-active device. For VIPRION systems that are not provisioned for vCMP, each chassis must have the same number of blades in the same slot numbers. For VIPRION systems provisioned for vCMP, each guest must be assigned to the same number of blades in the same slot numbers, with the same number of cores allocated per slot.

In addition to enabling connection mirroring on the virtual server, you must also assign the appropriate profiles to the virtual server. For example, if you want the BIG-IP system to mirror SSL connections, you must assign one or more SSL profiles to the virtual server.

Configuring connection mirroring within a VIPRION cluster

Using the BIG-IP® Configuration utility, you can configure mirroring among blades of a VIPRION® cluster within the same chassis.

Important: *Mirroring among blades within the same chassis applies to Fast L4 connections only. Also, mirroring can only occur between identical blade models.*

1. From a browser window, log in to the BIG-IP Configuration utility, using the cluster IP address.
2. On the Main tab, click **Device Management** > **Devices**.
   The Devices screen opens.
3. In the Device list, in the Name column, click the name of the device you want to configure.
4. From the Device Connectivity menu, choose Mirroring.
5. From the **Network Mirroring** list, select **Within Cluster**.
6. Click **Update**.

Configuring connection mirroring between VIPRION clusters

Before doing this task, you must enable connection mirroring on the relevant virtual server.

Using the BIG-IP® Configuration utility, you can configure connection mirroring between two VIPRION® or vCMP® clusters as part of your high availability setup:

- When you configure mirroring on a VIPRION system where vCMP is not provisioned (a bare-metal configuration), an active traffic group on one chassis mirrors its connections to the next-active chassis in the device group.
- When you configure mirroring on a vCMP guest, an active traffic group mirrors its connections to its next-active guest in another chassis.

Important: *Connection mirroring requires that both devices have identical hardware platforms (chassis and blades).*

Important: *You must perform this task locally on every device (chassis or vCMP guest) in the device group. For VIPRION systems with bare-metal configurations (no vCMP provisioned), each chassis must contain the same number of blades in the same slot numbers. For VIPRION systems provisioned for vCMP, each guest must reside on a separate chassis, be assigned to the same number of blades in the same slot numbers, and have the same number of cores allocated per slot.*

1. From a browser window, log in to the BIG-IP Configuration utility, using the cluster IP address.
2. On the Main tab, click **Device Management** > **Devices**.
   The Devices screen opens.
3. In the Device list, in the Name column, click the name of the device you want to configure.
4. From the Device Connectivity menu, choose Mirroring.
5. From the **Network Mirroring** list, select **Between Clusters**.
6. Click **Update**.

Legal Notices

Legal notices

Publication Date

This document was published on May 18, 2017.

Publication Number

MAN-0312-08

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

N

R

S

T

U

V