BIG-IP® Systems: Upgrading Software

Version 13.0

Table of Contents

Upgrading Version 11.x or 12.x BIG-IP Software

Introduction to upgrading version 11.x, or later, BIG-IP software

Version 11.x, or later, BIG-IP® systems are typically configured to employ the functionality of a device group. When you upgrade version 11.x, or later, BIG-IP software for a BIG-IP system device group, to the new version software, you can use a simple sequence of steps to successfully upgrade each device within the device group. The following steps enable you to prepare for a software upgrade, perform the upgrade, and then verify that the upgrade successfully completed.

1. Preparing BIG-IP modules for an upgrade
2. Preparing BIG-IP device groups for an upgrade
3. Upgrading each device within the device group
4. Changing states of the traffic groups
5. Configuring HA groups (if applicable)
6. Configuring module-specific settings
7. Verifying the software upgrade for the device group

Note: *For BIG-IP devices running version 12.1.1, or later, you can migrate the existing user configuration set (UCS) file from the version 12.1.1, or later, device to a new device running version 12.1.1, or later. For details, please refer to K82540512: Overview of the UCS archive platform-migrate option in the AskF5™ knowledge base at* `http://support.f5.com`.

Overview: Upgrading a version 11.x, or later, BIG-IP device group

A BIG-IP® system device group for version 11.x, or later, includes two or more BIG-IP systems, with one or more traffic groups operating in active state. In this example, a version 11.x, or later, device group includes one BIG-IP system with traffic-group-1 operating in active state (Device A), one BIG-IP system with traffic-group-2 operating in active state (Device B), and one BIG-IP system with traffic-group-3 operating in active state (Device C).

Important: *If your version 11.x device group includes HA groups, note that an HA group applies to the respective device in version 11.0 through 11.4.x, whereas an HA group applies to a traffic group on the device in version 11.5, and later.*

Note: *When upgrading a device group from version 11.x, or later, software to the latest version software, mirroring does not function until all devices in the device group complete rebooting to the latest version. F5 Networks® recommends upgrading software during a scheduled maintenance window, to minimize traffic disruption when devices run different software versions.*

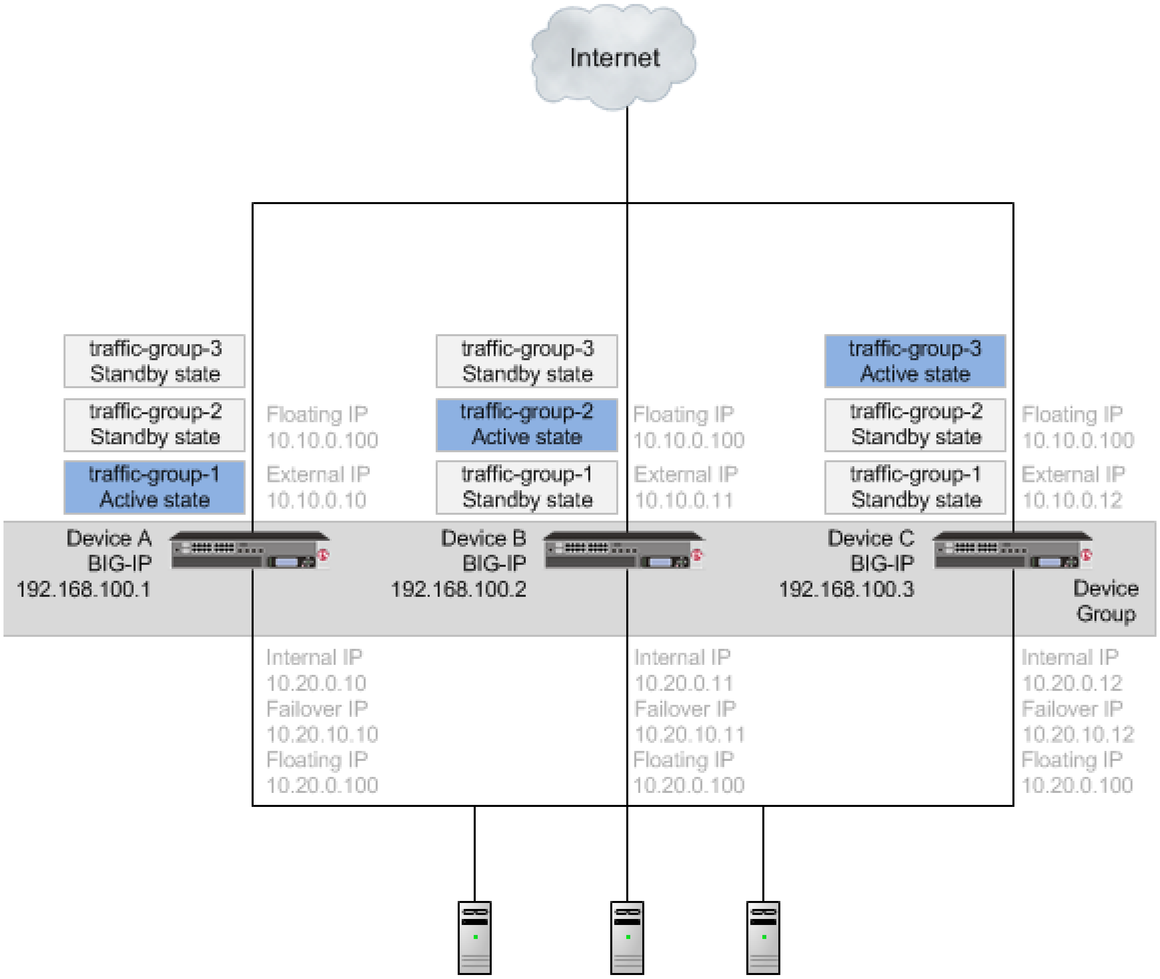

Figure 1: A version 11.x, or later, device group

When upgrading an 11.x, or later, device group to the new version software, you first need to prepare your devices. After preparing the devices, you force Device A to offline state, and install the new version software onto Device A. When you finish the installation of the new version software onto Device A, the traffic groups remain in standby state on Device A, and in active state on Device B and Device C.

Important: *Once Device A reboots, if the BIG-IP system is configured to use a network hardware security module (HSM), you must reinstall network HSM client software on Device A before upgrading Device B, to ensure that traffic groups using the network HSM function properly.*

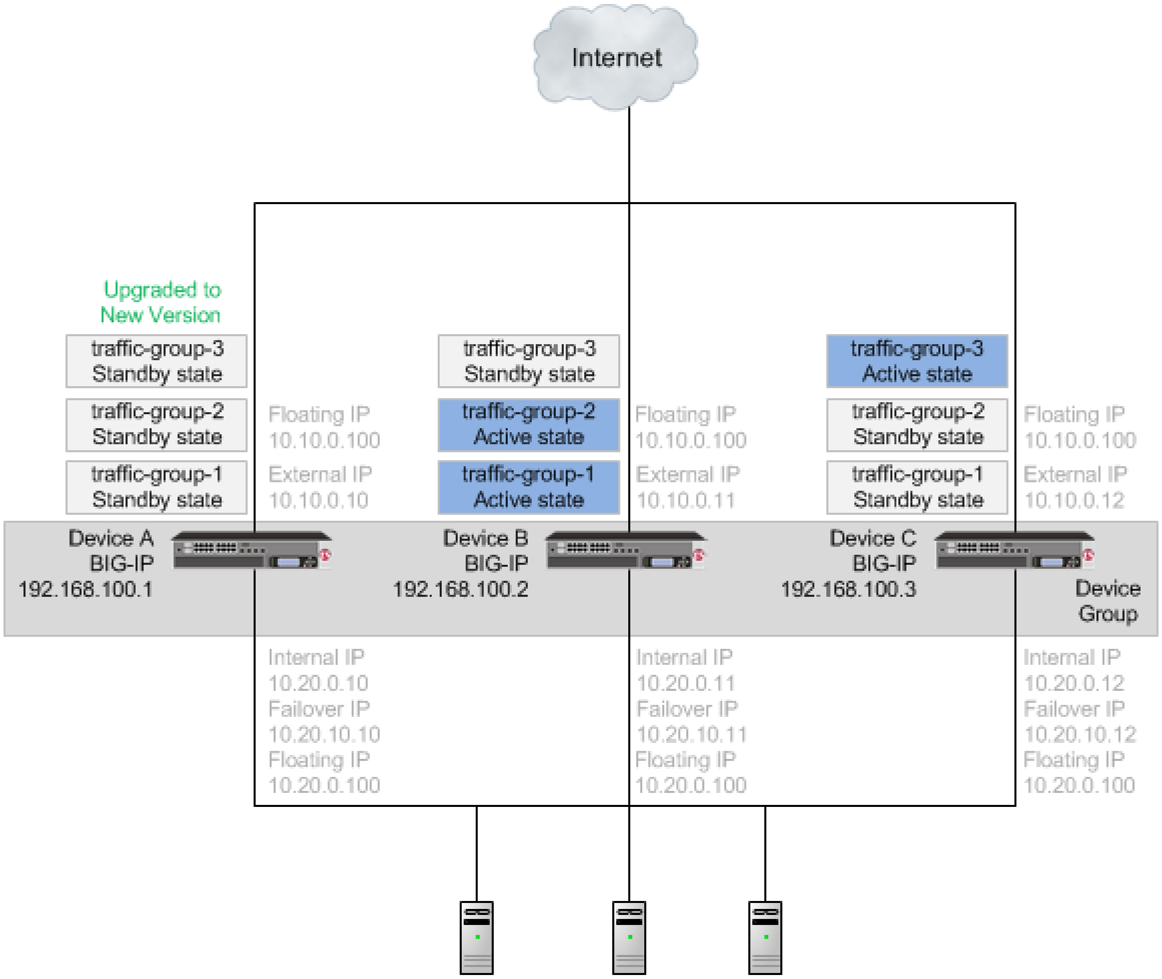

Figure 2: A device group with Device A upgraded to the new version software, and traffic groups in standby state

With the new version software installed on Device A and all traffic groups in standby state, you force Device B to offline state, changing the traffic groups on Device A to active state so that they can pass traffic. You can then install the new version software onto Device B, and reboot Device B to the location of the new version software image.

Important: *Once Device B reboots, if the BIG-IP system is configured to use a network HSM, you must reinstall network HSM client software on Device B before upgrading Device C, to ensure that traffic groups using the network HSM function properly.*

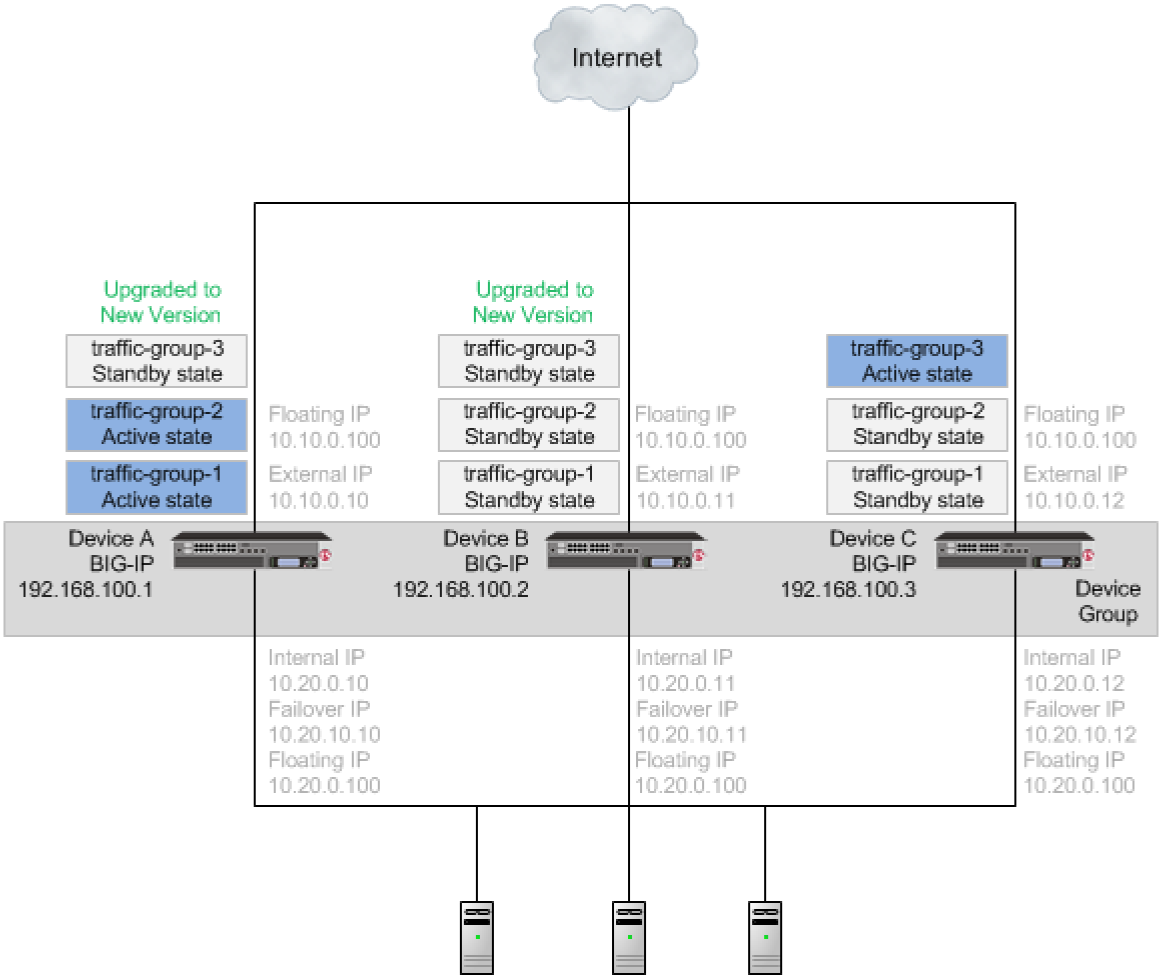

Figure 3: A device group with Device B upgraded to the new version software, and traffic groups in standby state

Once Device B reboots, you can force Device C to offline state, making traffic-group-3 active on Device B. When you complete upgrading Device C to the new version software and reboot Device C, the BIG-IP configuration includes traffic-group-1 and traffic-group-2 in active state on Device A, traffic-group-3 in active state on Device B, and a device group that includes all devices. If you use HA groups, observe that the HA group on Device A, Device B, and Device C applies to each traffic group.

Important: *Once Device C reboots, if the BIG-IP system is configured to use a network HSM, you must reinstall network HSM client software on Device C, to ensure that traffic groups using the network HSM function properly.*

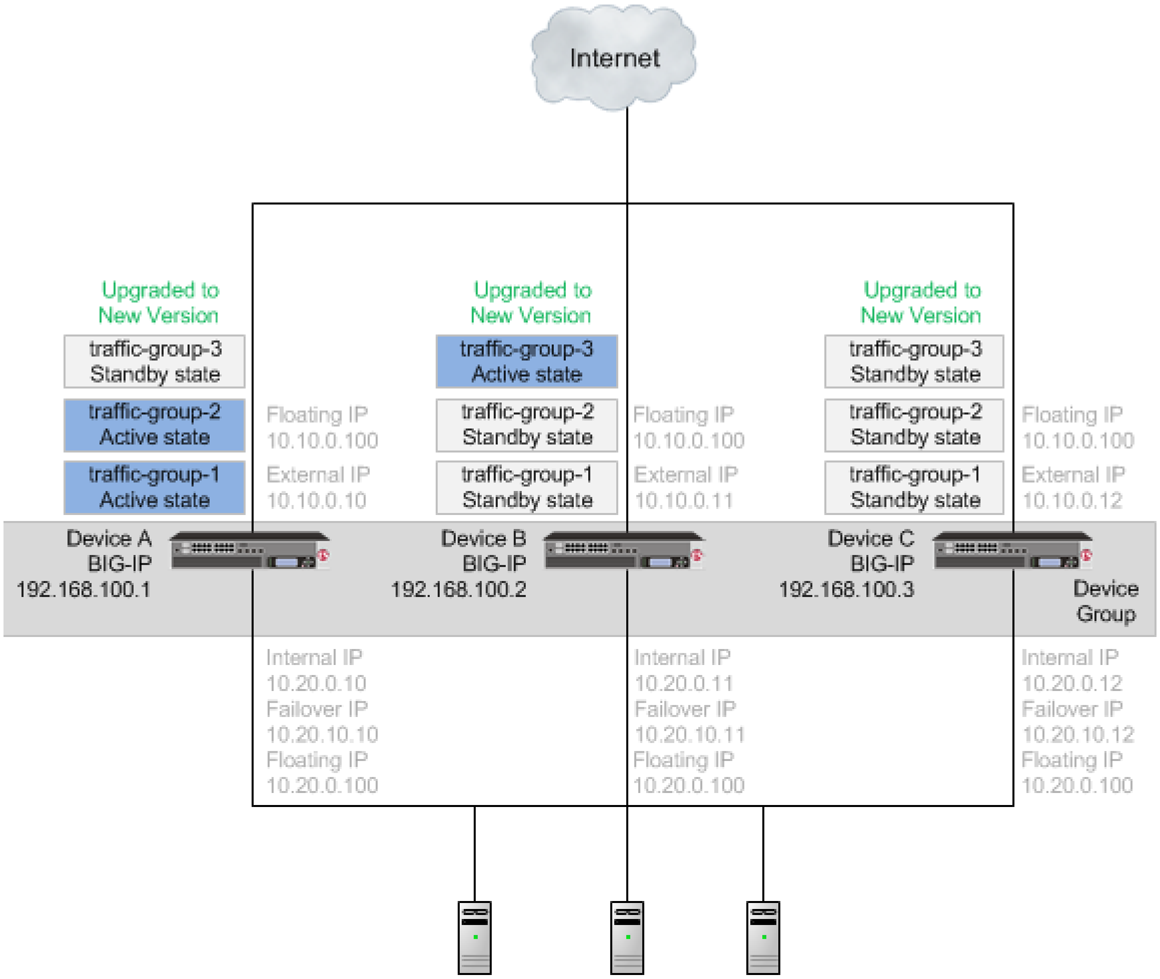

Figure 4: A device group with all devices upgraded to the new version software

Once each device is upgraded to the new version software, you can reconfigure the traffic groups to become active on the devices that you want by forcing the active traffic group on a device to standby state. When forcing the traffic group to standby state, you can target the device upon which you want that traffic group to run in active state. For example, you can force traffic-group-2 on Device A into standby state, and into active state on Device B, and then force traffic-group-3 on Device B into standby state, and into active state on Device C. Additionally, if you use HA groups, you can create a unique HA group for each traffic group on each device.

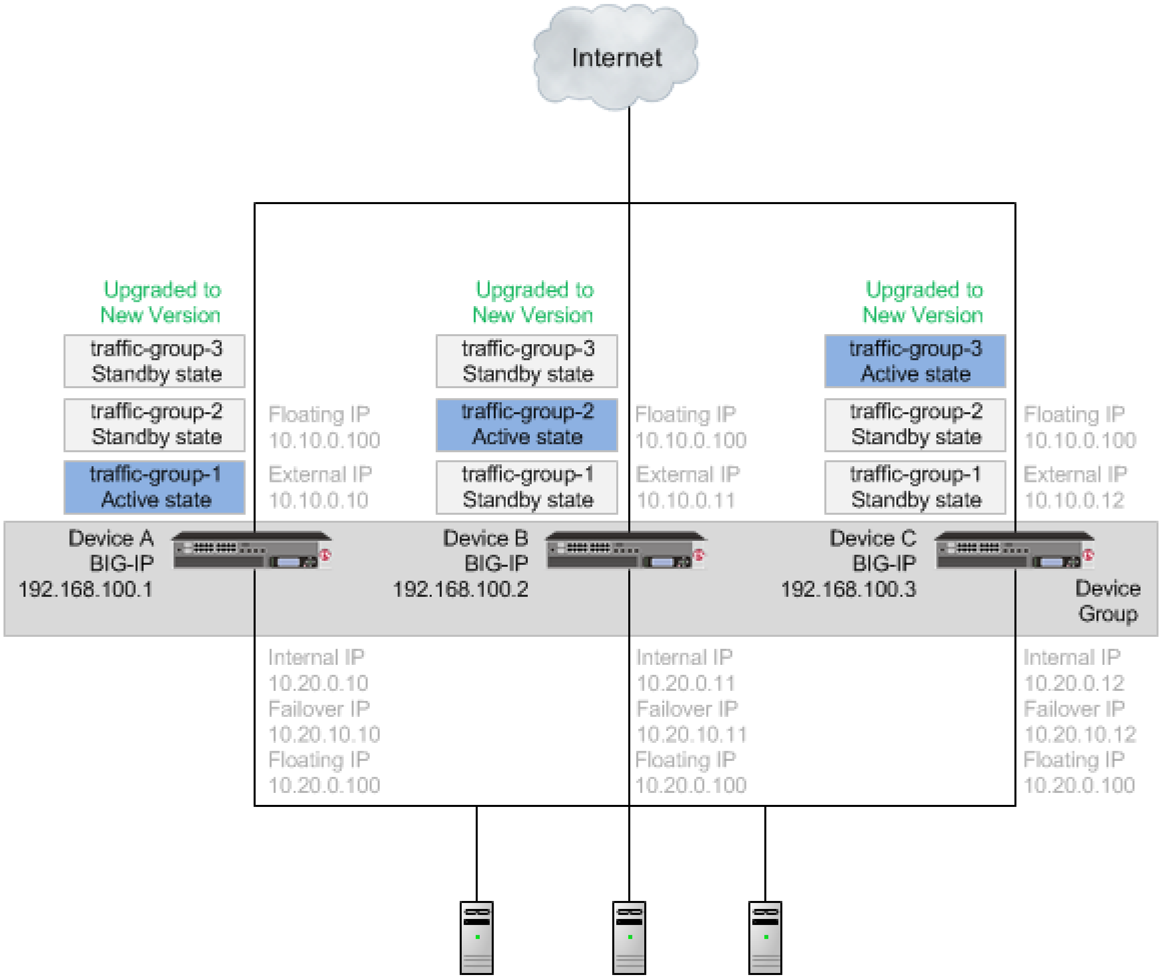

Figure 5: A device group with an active traffic group on each device

Summary of tasks

Task	Description
Preparing the devices in the device group	In preparing to upgrade the BIG-IP systems to the new version software, you need to understand any specific configuration or functional changes from the previous version, and prepare the systems. You also download the new version of software from the AskF5™ web site (`http://support.f5.com/kb/en-us.html`) and import the files onto each device.
Upgrading Device A	When you complete preparation of Device A, you can force that device to offline state, changing those traffic groups to active state on another device in the traffic group, and then upgrade the software on Device A. ***Important:*** *Once Device A reboots, if the BIG-IP system is configured to use a network HSM, you must reinstall network HSM client software on Device A before upgrading Device B, to ensure that traffic groups using the network HSM function properly.*
Upgrading Device B	When you complete preparation of Device B, you can force that device to offline state, changing those traffic groups to active state on another device in the traffic group, and then upgrade the software on Device B.

Task	Description
	Important: *Once Device B reboots, if the BIG-IP system is configured to use a network HSM, you must reinstall network HSM client software on Device B before upgrading Device C, to ensure that traffic groups using the network HSM function properly.*
Upgrading Device C	When you complete preparation of Device C, you can force that device to offline state, changing those traffic groups to active state on another device in the traffic group, and then upgrade the software on Device C. ***Important:*** *Once Device C reboots, if the BIG-IP system is configured to use a network HSM, you must reinstall network HSM client software on Device C to ensure that traffic groups using the network HSM function properly.*
Changing states of traffic groups	When you finish upgrading all of the devices, you can restore the configuration of active traffic groups on each device.
Verifying the upgrade	Finally, you should verify that the BIG-IP device group is functioning properly.
Configuring HA groups	When you finish upgrading a device, the HA group on the device (in version 11.5, and later) applies to a traffic group, as opposed to the device. You can create a unique HA group for each traffic group on each device, as necessary.
Configuring module-specific settings	According to your understanding of the configuration and functional changes from the previous version, you can reconfigure any customized module settings.

DSC components

Device service clustering (DSC®) is based on a few key components.

Devices

A *device* is a physical or virtual BIG-IP® system, as well as a member of a local trust domain and a device group. Each device member has a set of unique identification properties that the BIG-IP system generates. For device groups configured for failover, it is important that the device with the smallest capacity has the capacity to process all traffic groups. This ensures application availability in the event that all but one device in the device group become unavailable for any reason.

Device groups

A *device group* is a collection of BIG-IP devices that trust each other and can synchronize, and sometimes fail over, their BIG-IP configuration data. A *Sync-Failover* device group contains devices that synchronize configuration data and support traffic groups for failover purposes when a device becomes unavailable. The BIG-IP system supports either homogeneous or heterogeneous hardware platforms within a device group.

Important: *BIG-IP module provisioning must be equivalent on all devices within a device group. For example, module provisioning is equivalent when all device group members are provisioned to run BIG-IP® Local Traffic Manager™ (LTM®) and BIG-IP® Application Security Manager™ (ASM™) only. Maintaining equivalent module provisioning on all devices ensures that any device in the device group can process module-specific application traffic in the event of failover from another device.*

Traffic groups

A *traffic group* is a collection of related configuration objects (such as a virtual IP address and a self IP address) that run on a BIG-IP device and process a particular type of application traffic. When a

BIG-IP device becomes unavailable, a traffic group can float to another device in a device group to ensure that application traffic continues to be processed with little to no interruption in service.

Device trust and trust domains

Underlying the success of device groups and traffic groups is a feature known as device trust. *Device trust* establishes trust relationships between BIG-IP devices on the network, through mutual certificate-based authentication. A *trust domain* is a collection of BIG-IP devices that trust one another and is a prerequisite for creating a device group for config sync and failover operations. The trust domain is represented by a special system-generated and system-managed device group named `device_trust_group`, which is used to synchronize trust domain information across all devices.

Folders

Folders are containers for the configuration objects on a BIG-IP device. For every administrative partition on the BIG-IP system, there is a high-level folder. At the highest level of the folder hierarchy is a folder named `root`. The BIG-IP system uses folders to affect the level of granularity to which it synchronizes configuration data to other devices in the device group.

About traffic groups

Traffic groups are the core component of failover. A *traffic group* is a collection of related configuration objects, such as a floating self IP address, a floating virtual IP address, and a SNAT translation address, that run on a BIG-IP® device. Together, these objects process a particular type of application traffic on that device.

When a BIG-IP® device goes offline, a traffic group floats (that is, fails over) to another device in the device group to make sure that application traffic continues to be processed with minimal interruption in service.

A traffic group is first active on the device you created it on. If you want an active traffic group to be active on a different device than the one you created it on, you can force the traffic group to switch to a standby state. This causes the traffic group to fail over to (and become active on) another device in the device group. The device it fails over to depends on how you configured the traffic group when you created it.

Note: *A Sync-Failover device group can support a maximum of 127 floating traffic groups.*

About forcing a device offline

You can force a BIG-IP® device into an offline state, which stops that device from processing or responding to local traffic connections. When the device is in offline state, you can upgrade the software on that device or perform maintenance on that device.

When the BIG-IP system is forced offline, it terminates existing connections to local traffic objects, such as virtual servers, SNATs, and so on. In the forced offline state, the BIG-IP system does not allow new connections.

For BIG-IP systems running software version 11.1.0 and later, the Force Offline status persists through system reboots and upgrades. For BIG-IP systems running software versions earlier than 11.1.0, the Force Offline status does not persist through system reboots.

The BIG-IP system allows administrative connections to the management address to continue, but handles administrative connections to self IP addresses differently, depending on the platform:

- On appliance systems, the system maintains connections to self IP addresses.
- On VIPRION® systems, the system terminates connections to self IP addresses, and does not allow new connections.

***Note:** When you force a chassis system offline, the Traffic Management Microkernel (TMM) interfaces remain configured until the unit is rebooted. If the chassis is rebooted while Force Offline is enabled, the system marks all TMM interfaces as `Uninitialized` or `Missing`. This behavior is by design. The system will not attempt to initialize and bring up TMM interfaces while the system is in the offline state.*

When you force VIPRION platforms offline, make sure to manage the system by using the management port or console. The system terminates connections to self IP addresses when you force the platform offline.

You will want to force the standby devices offline before you change the redundancy state (such as resetting the device trust for a device group). Forcing standby devices into offline state prevents a standby device from unexpectedly becoming active.

Task summary

The upgrade process involves preparation of the BIG-IP® devices (Device A, Device B, and Device C) configured in device group, followed by the installation and verification of the new version software on each device. When you upgrade each device, you perform several tasks. Completing these tasks results in a successful upgrade to the new version software on all BIG-IP devices, with the device group configured properly.

Preparing BIG-IP modules for an upgrade from version 11.x, or later
Preparing RAID drives for an upgrade
Preparing BIG-IP device groups for an upgrade
Upgrading the Device A system
Upgrading the Device B system
Upgrading the Device C system
Changing states of the traffic groups
Verifying a BIG-IP device group upgrade

Preparing BIG-IP modules for an upgrade from version 11.x, or later

Before you upgrade the BIG-IP® system from version 11.x, or later, to the new version, you might need to manually prepare settings or configurations for specific modules.

Application Acceleration Manager preparation

BIG-IP® Application Acceleration Manager™ (AAM®) modules require specific preparation tasks and changes to upgrade from version 11.x, or later, to the new version software. No additional configuration is required after completing the upgrade to the new version software.

Preparation activities

Before you upgrade the BIG-IP® Application Acceleration Manager™ (AAM®) modules from version 11.x, or later, to the new version software, you need to prepare the systems, based on your configuration. The following table summarizes the applicable tasks that you need to complete.

Feature or Functionality	Preparation Task
Unpublished policies	You must publish any policies that you want to migrate to the new version software. Only published policies are migrated into the new version software.

Advanced Firewall Manager system preparation

The BIG-IP® Advanced Firewall Manager™ (AFM™) system does not require specific preparation when upgrading from version 11.x, or later, to the new version software. No additional configuration is required after completing the upgrade to the new version software.

Access Policy Manager system preparation

The Access Policy Manager® system does not require specific preparation when upgrading from version 11.x, or later, to the new version software. However, additional configuration might be required after completing the upgrade to the new version software.

Supported high availability configuration for Access Policy Manager

Access Policy Manager is supported in an active-standby configuration with two BIG-IP® systems only.

Important: *Access Policy Manager is not supported in an active-active configuration.*

Post-upgrade activities

When you finish upgrading to the new version software, you should consider the following feature or functionality changes that occur for the Access Policy Manager systems. Depending on your configuration, you might need to perform these changes after you upgrade your systems.

Feature or Functionality	Description
Sessions	All users currently logged in while the upgrade occurs will need to log in again.
Authentication agents and SSO methods	If you have deployments using ActiveSync or Outlook Anywhere, where the domain name is part of the user name, you should enable the **Split domain from username** option in the login page agent if the authentication method used in the access policy requires only the user name for authentication.

Application Security Manager system preparation

The BIG-IP® Application Security Manager™ (ASM™) system does not require specific preparation when upgrading from version 11.x, or later, to the new version software. No additional configuration is required after completing the upgrade to the new version software.

What to expect after upgrading a redundant system

If you update two redundant systems that are running as an active-standby pair with BIG-IP Application Security Manager (ASM) and BIG-IP® Local Traffic Manager™ (LTM®) provisioned, the system maintains the active-standby status and automatically creates a Sync-Failover device group and a traffic group containing both systems. The device group is enabled for BIG-IP ASM (because both systems have ASM provisioned).

You can manually push or pull the updates (including BIG-IP LTM and ASM configurations and policies) from one system to the other (**Device Management** > **Overview**, click the name of a device, and then choose **Sync Device to Group** or **Sync Group to Device**).

Global Traffic Manager system preparation and configuration

BIG-IP® Global Traffic Manager systems require specific preparation and configuration when upgrading from version 11.x, or later, to the new version software.

Preparation activities

You should complete these activities before upgrading Global Traffic Manager systems from version 11.x, or later, to the new version software (BIG-IP® DNS).

***Important:** In BIG-IP version 12.0, BIG-IP Global Traffic Manager is renamed to BIG-IP DNS. After you upgrade, you will see the new name in the product and documentation.*

Activity	Instructions
Verify that the device certificates are current, and that expiration does not occur until after upgrading.	**1.** On the Main menu, click **System** > **Device Certificates** > **Device Certificate**. **2.** Verify the **Expires** date.
Disable configuration synchronization and DNS zone files synchronization. ***Note:** To use a backup UCS file without synchronizing the GTM configuration, disable synchronization. If synchronization is enabled, restoring the UCS backup file loads the configuration and initiates synchronization.*	**1.** On the Main menu, click **DNS** > **Settings** > **GSLB** > **General**. **2.** Clear the **Synchronize** check box. **3.** Clear the **Synchronize DNS Zone Files** check box.

Post-upgrade activities

You should complete these tasks after upgrading BIG-IP DNS systems from 11.x, or later, to the new version software.

***Important:** In BIG-IP version 12.0, BIG-IP Global Traffic Manager is renamed to BIG-IP DNS. After you upgrade, you will see the new name in the product and documentation.*

- From the command line, run the `big3d_install` script on the first BIG-IP DNS system that you upgraded, so that you can monitor other BIG-IP DNS systems.

  ***Important:** Run this script only once, only from the first BIG-IP DNS system that you upgraded. This step momentary degrades monitoring performance as new `big3d` agents start.*
- On each device, verify the configuration.
- On each device, test queries against listeners.
- On each device, verify iQuery® connections by using the `tmsh` command `tmsh show /gtm iquery all`.
- Enable synchronization on each device.
- Verify configuration synchronization by using a dummy test object; for example, by using an object that can be deleted after the configuration synchronization is verified as operational.

Link Controller system preparation

The BIG-IP® Link Controller™ (LC™) system does not require specific preparation when upgrading from version 11.x, or later, to the new version software. No additional configuration is required after completing the upgrade to the new version software.

Local Traffic Manager system preparation

The BIG-IP® Local Traffic Manager™ (LTM®) system does not require specific preparation when upgrading from version 11.x, or later, to the new version software. No additional configuration is required after completing the upgrade to the new version software.

HTTP Class profiles

F5 Networks® replaced the HTTP Class profile in BIG-IP® version 11.4.0, and later, with the introduction of the Local Traffic Policies feature. During an upgrade to BIG-IP version 11.4.0, if your configuration contains an HTTP Class profile, the BIG-IP system attempts to migrate the HTTP Class profile to an equivalent local traffic policy. For additional support information regarding the change of HTTP Class profiles to Local Traffic Policies, refer to SOL14409 on `www.askf5.com`.

Policy Enforcement Manager system preparation

The BIG-IP® Policy Enforcement Manager™ (PEM™) system does not require specific preparation when upgrading from version 11.x, or later, to the new version software. No additional configuration is required after completing the upgrade to the new version software.

Preparing RAID drives for an upgrade

If your configuration includes redundant array of independent disks (RAID) drives, you need to verify that the RAID drives are ready for upgrading. If a RAID drive shows errors before upgrading, you will want to contact F5 customer support to resolve the errors before initiating the upgrade.

1. Open the Traffic Management Shell (tmsh).
   `tmsh`
   This starts `tmsh` in interactive shell mode and displays the `tmsh` prompt: `(tmos)#`.
2. Verify the health of RAID disks, ensuring that the drives are not failed or undefined.

   `(tmos)# show sys raid`

```
Sys::Raid::Array: MD1
--------------------
Size (MB) 305245

Sys::Raid::ArrayMembers
Bay ID Serial Number Name Array Member Array Status
---------------------------------------------------------
1 WD-WCAT18586780 HD2 yes failed
2 WD-WCAT1E733419 HD1 yes ok
```

   In this example, the array is labeled MD1 and disk HD2 indicates an error.
3. Verify `Current_Pending_Sector` data displays a `RAW_VALUE` entry of less than `1` on RAID systems.

Option	Description
For version 11.4.0, and later	Run the platform check utility: `(tmos)# run util platform_check`
For version 11.3.x, and earlier	At the command line, run the smartctl utility: `smartctl -t long -d ata /dev/<sda|sdb|hda|hdc>`

```
197 Current_Pending_Sector  0x0032  200  200  000  Old_age  Always  -  0
```

   In this example, the `RAW_VALUE` entry is `0`.
4. Verify that no known issues appear in the following log files.

- Check `/var/log/user.log` for LBA messages indicating failure to recover, for example, `recovery of LBA:226300793 not complete`.
- Check `/var/log/kern.log` for ATA error entries.

The health of all RAID drives is assessed, enabling you to resolve any issues before proceeding with the BIG-IP® software upgrade.

Preparing BIG-IP device groups for an upgrade

The following prerequisites apply when you upgrade BIG-IP® device groups from version 11.x, or later, to the new version.

- The BIG-IP systems (Device A, Device B, and Device C) are configured as a device group.
- Each BIG-IP device is running the same version of 11.x, or later, software.
- The BIG-IP version 11.x, or later, devices are the same model of hardware.

When you upgrade a BIG-IP device group from version 11.x, or later, to the new version, you begin by preparing the devices.

***Note:** If you prefer to closely observe the upgrade of each device, you can optionally connect to the serial console port of the device that you are upgrading.*

1. For each device, complete the following steps to prepare the configuration and settings.
   a) Examine the Release Notes for specific configuration requirements, and reconfigure the systems, as necessary.
   b) Examine the Release Notes for specific changes to settings that occur when upgrading from version 11.x, or later, to the new version, and complete any in-process settings.
2. From the device that is running the latest configuration, synchronize the configuration to the devices in the device group.

Option	Description
For version 11.2, and earlier.	**1.** On the Main menu, click **Device Management** > **Device Groups**. A list of device groups appears. **2.** In the Group Name column, click the name of a device group. **3.** On the menu bar, click **ConfigSync**. **4.** Click **Synchronize To Group**.
For version 11.3, and later.	**1.** On the Main menu, click **Device Management** > **Overview**. A message appears for the Status Message. **2.** In the Devices area of the screen, in the Sync Status column, click the device that shows a sync status of `Changes Pending`. **3.** Click **Synchronize Device to Group**.

3. For each device, create a QKView file, and upload it to iHealth™.
   a) On the Main menu, click **System** > **Support**.

      The Support screen opens.
   b) Select the **QKView** check box.
   c) Click **Start**.

      The BIG-IP system creates a QKView file.
   d) Click **Download Snapshot File**, and click **Save**.

      The BIG-IP system downloads the QKView file, named `case_number_###_support_file.qkview`, into the browser's download folder.
   e) Rename the QKView file to include a case number and an identifier.

An example of a renamed file is: `c123456_A_support_file.qkview`.

f) Go to `https://ihealth.f5.com`, and log in using your F5 WebSupport credentials.

g) Click **Upload**.

h) Click **Browse**, navigate to the QKView file in the download folder, and then click **Open**.

i) Click **Upload QKView(s)**.

4. For each device, create a backup file.

a) Access the `tmsh` command line utility.

b) At the prompt, type `save /sys ucs /shared/filename.ucs`.

c) Copy the backup file to a safe location on your network.

Note: *For additional support information about backing up and restoring BIG-IP system configuration files, refer to SOL11318 on* `www.askf5.com`*.*

5. Download either the latest BIG-IP system hotfix image file, if available, or the new version software image file from the AskF5 downloads web site (`http://support.f5.com/kb/en-us.html`) to a preferred location.

Important: *If you want to upgrade to a BIG-IP system hotfix image file that applies to incremental major version software, you must download the incremental version software and the hotfix image file. For example, if you want to upgrade from BIG-IP version 11.x software to a 12.x hotfix image file, then you must download a version 12.x software image file and the hotfix image file.*

6. Import either the latest BIG-IP system hotfix image file, if available, or the new version software upgrade image file to each device.

Option	Description
Import the latest BIG-IP system hotfix image and SIG file	**1.** On the Main menu, click **System** > **Software Management** > **Hotfix List** > **Import**. **2.** Click **Browse**, locate and click the SIG file (Hotfix-BIGIP-hf-xx.x.x.x.x.xxxx.HFx.iso.384.sig), click **Open**, and click **Import**. **3.** Click **Browse**, locate and click the image file, click **Open**, and click **Import**. **4.** When the hotfix image file completes uploading to the BIG-IP device, click **OK**. A link to the image file appears in the Software Image list.
Import the new version software image and SIG file	**1.** On the Main menu, click **System** > **Software Management** > **Image List** > **Import**. **2.** Click **Browse**, locate and click the SIG file (BIGIP-13.x.x.x.x.xxxx.iso.384.sig), click **Open**, and click **Import**. **3.** Click **Browse**, locate and click the upgrade image file, click **Open**, and click **Import**. ***Note:*** *BIG-IP version 13.x, and later, provides upgrade and recovery image files. An upgrade image file (for example, BIGIP-13.x.x.x.x.xxxx.iso) omits End User Diagnostics (EUD) software, which includes tests that report on hardware components. A recovery image file (for example, BIGIP-RECOVERY-13.x.x.x.x.xxx.iso) includes EUD software.* **4.** When the software image file completes uploading to the BIG-IP device, click **OK**. A link to the image file appears in the Software Image list.

7. (Optional) Verify the integrity of the imported software image file.

Option	Description
Use SIG verification (recommended)	**1.** At the command line, determine the filename of the applicable public key file. Example: `# ls /usr/lib/install/archive.pubkey*pem`. The list of `archive.pubkey` files appears. **2.** Using the openssl utility, verify the integrity of the imported software image file. Example: `# openssl dgst -sha384 -verify usr/lib/install/ archive.pubkey.xxxxxxxxx.pem -signature shared/images/ BIGIP-13.x.x.x.x.xxxx.iso.384.sig shared/images/ BIGIP-13.x.x.x.x.xxxx.iso` ***Note:*** *You must use openssl version 1.0.0, or later. Type* `openssl version` *at the command line to determine the version.* The openssl utility verifies the integrity of the software image file and displays the results. # openssl dgst -sha384 -verify usr/lib/install/ archive.pubkey.xxxxxxxxx.pem -signature shared/images/ BIGIP-13.x.x.x.x.xxxx.iso.384.sig shared/images/ BIGIP-13.x.x.x.x.xxxx.iso Verified OK
Use an MD5 checksum	• Using a tool or utility that computes an md5 checksum, you can verify the integrity of the BIG-IP system latest hotfix `.iso` file or new version `.iso` file.

8. If the BIG-IP system is configured to use a network hardware security module (HSM), the HSM client software must be available for reinstallation.

   Important: *Make sure that the available version of HSM client software supports the new version of BIG-IP software.*

The BIG-IP devices are prepared to install the latest hotfix or new version software.

Upgrading the Device A system

The following prerequisites apply for this task.

- Each device must be prepared to upgrade Device A with the new version software.
- Either the latest hotfix image file, if available, or the new version software image file is downloaded and accessible.

Important: *If you want to upgrade to a BIG-IP® system hotfix image file that applies to incremental major version software, you must install the incremental version software before installing the hotfix image file. For example, if you want to upgrade from BIG-IP version 11.x software to a 12.x hotfix image file, then you must install a version 12.x software image file before you install the hotfix image file.*

After you prepare each device for upgrading the software, you force the device offline, reactivate the software license, and install the new version software onto Device A.

1. Force Device A to offline state.

a) On the Main menu, click **Device Management** > **Devices**.
b) Click the name of Device A.
The device properties screen opens.
c) Click **Force Offline**.

Device A changes to offline state.

> ***Important:*** *Once Device A changes to offline state, ensure that traffic passes normally for all active traffic groups on the other devices.*

> ***Note:*** *When* ***Force Offline*** *is enabled, make sure to manage the system using the management port or console. Connections to self IP addresses are terminated when* ***Force Offline*** *is enabled.*

2. Reactivate the software license.

a) On the Main menu, click **System** > **License**.
b) Click **Re-activate**.
c) For the **Activation Method** setting, select the **Automatic (requires outbound connectivity)** option.
d) Click **Next**.
The BIG-IP software license renews automatically.
e) Click **Continue**.

3. Install either the latest hotfix image, if available, or the new version software.

> ***Important:*** *If you want to upgrade to a BIG-IP system hotfix image file that applies to incremental major version software, you must install the incremental version software before installing the hotfix image file. For example, if you want to upgrade from BIG-IP version 11.x software to a 12.x hotfix image file, then you must install a version 12.x software image file before you install the hotfix image file.*

Option	Description
Install the latest hotfix image	**1.** On the Main menu, click **System** > **Software Management** > **Hotfix List**. **2.** In the Available Images area, select the check box for the hotfix image, and click **Install**. The Install Software Hotfix popup screen opens. **3.** From the **Volume set name** list, select the location of the new version software volume to install the hotfix image, and click **Install**. ***Important:*** *In the* ***Install Status*** *list for the specified location, a progress bar indicates the status of the installation. Ensure that installation successfully completes, as indicated by the progress bar, before proceeding.* ***Note:*** *The format for a volume set name is lower case only, alphanumeric with hyphenation, and limited to 32 characters.*
Install the new version software	**1.** On the Main menu, click **System** > **Software Management** > **Image List**. **2.** In the Available Images area, select the check box for the new version software image, and click **Install**. The Install Software Image popup screen opens. **3.** From the **Volume set name** list, select a location to install the image, and click **Install**.

Option	Description
	Important: *In the* ***Install Status*** *list for the specified location, a progress bar indicates the status of the installation. Ensure that installation successfully completes, as indicated by the progress bar, before proceeding.* ***Note:*** *The format for a volume set name is lower case only, alphanumeric with hyphenation, and limited to 32 characters.*

4. Reboot the device to the location of the installed new software image.

Note: *When upgrading a device group from version 11.x, or later, software to the latest version software, mirroring does not function until all devices in the device group complete rebooting to the latest version. F5 Networks® recommends upgrading software during a scheduled maintenance window, to minimize traffic disruption when devices run different software versions.*

Option	Description
Reboot from version 11.3.0, or earlier	**1.** On the Main menu, click **System** > **Software Management** > **Boot Locations**. **2.** In the Boot Location list, click the boot location of the installed new software image. ***Note:*** *Upgrading from version 11.3.0, or earlier, automatically installs the configuration of that version to the new boot location.* **3.** Click **Activate**. Device A reboots to the new software image boot location in offline state. ***Note:*** *If the device appears to be taking a long time to reboot, do not cycle the power off and on. Instead, verify the status of the device by connecting to its serial console port. The device might be performing firmware upgrades.*
Reboot from version 11.4.0, or later	**1.** On the Main menu, click **System** > **Software Management** > **Boot Locations**. **2.** In the **Boot Location** list, click the boot location of the installed new software image. **3.** From the **Install Configuration** list, select **Yes**. The **Source Volume** list appears. **4.** From the **Source Volume** list, select the location of the configuration to install when activating the boot location of the new software image. For example, for an installation of a new software image on HD1.3, selecting **HD1.2:11.6.0** installs the version 11.6.0 configuration. **5.** Click **Activate**. Device A reboots to the new software image boot location in offline state. ***Note:*** *If the device appears to be taking a long time to reboot, do not cycle the power off and on. Instead, verify the status of the device by connecting to its serial console port. The device might be performing firmware upgrades.*

5. If the BIG-IP system is configured to use a network hardware security module (HSM), reinstall and configure the HSM client software.

Important: *You must reinstall network HSM client software on this device before upgrading another device in the device group, to ensure that traffic groups using the network HSM function properly.*

6. Release Device A from offline state.

a) On the Main menu, click **Device Management** > **Devices**.
b) Click the name of Device A.
The device properties screen opens.
c) Click **Release Offline**.
Device A changes to standby state.

The new version of BIG-IP® software is installed on Device A, with all traffic groups in standby state.

Upgrading the Device B system

The following prerequisites apply in upgrading Device B.

- Device B must be prepared to upgrade the software to new version software.
- Either the latest hotfix image file, if available, or the new version software image file is downloaded and accessible.

Important: *If you want to upgrade to a BIG-IP® system hotfix image file that applies to incremental major version software, you must install the incremental version software before installing the hotfix image file. For example, if you want to upgrade from BIG-IP version 11.x software to a 12.x hotfix image file, then you must install a version 12.x software image file before you install the hotfix image file.*

- If the BIG-IP system is configured to use a network hardware security module (HSM), you must reinstall network HSM client software on Device A before upgrading Device B, to ensure that traffic groups using the network HSM function properly.
- Device A (the new version BIG-IP® device) is in standby state.

After you prepare Device B for upgrading the software, you force the device offline, reactivate the software license, and install the new version software.

1. Force Device B to offline state.
   a) On the Main menu, click **Device Management** > **Devices**.
   b) Click the name of Device B.
   The device properties screen opens.
   c) Click **Force Offline**.

   Device B changes to offline state.

   Important: *Once Device B changes to offline state, ensure that Device A passes traffic normally for all active traffic groups.*

   Note: *When* ***Force Offline*** *is enabled, make sure to manage the system using the management port or console. Connections to self IP addresses are terminated when* ***Force Offline*** *is enabled.*

2. Reactivate the software license.
   a) On the Main menu, click **System** > **License**.
   b) Click **Re-activate**.
   c) For the **Activation Method** setting, select the **Automatic (requires outbound connectivity)** option.
   d) Click **Next**.
   The BIG-IP software license renews automatically.
   e) Click **Continue**.
3. Install either the latest hotfix image, if available, or the new version software.

***Important:** If you want to upgrade to a BIG-IP system hotfix image file that applies to incremental major version software, you must install the incremental version software before installing the hotfix image file. For example, if you want to upgrade from BIG-IP version 11.x software to a 12.x hotfix image file, then you must install a version 12.x software image file before you install the hotfix image file.*

Option	Description
Install the latest hotfix image	1. On the Main menu, click **System** > **Software Management** > **Hotfix List**. 2. In the Available Images area, select the check box for the hotfix image, and click **Install**. The Install Software Hotfix popup screen opens. 3. From the **Volume set name** list, select the location of the new version software volume to install the hotfix image, and click **Install**. ***Important:** In the **Install Status** list for the specified location, a progress bar indicates the status of the installation. Ensure that installation successfully completes, as indicated by the progress bar, before proceeding.* ***Note:** The format for a volume set name is lower case only, alphanumeric with hyphenation, and limited to 32 characters.*
Install the new version software	1. On the Main menu, click **System** > **Software Management** > **Image List**. 2. In the Available Images area, select the check box for the new version software image, and click **Install**. The Install Software Image popup screen opens. 3. From the **Volume set name** list, select a location to install the image, and click **Install**. ***Important:** In the **Install Status** list for the specified location, a progress bar indicates the status of the installation. Ensure that installation successfully completes, as indicated by the progress bar, before proceeding.* ***Note:** The format for a volume set name is lower case only, alphanumeric with hyphenation, and limited to 32 characters.*

4. Reboot the Device B to the location of the installed new software image.

***Note:** When upgrading a device group from version 11.x, or later, software to the latest version software, mirroring does not function until all devices in the device group complete rebooting to the latest version. F5 Networks® recommends upgrading software during a scheduled maintenance window, to minimize traffic disruption when devices run different software versions.*

Option	Description
Reboot from version 11.3.0, or earlier	1. On the Main menu, click **System** > **Software Management** > **Boot Locations**. 2. In the Boot Location list, click the boot location of the installed new software image. ***Note:** Upgrading from version 11.3.0, or earlier, automatically installs the configuration of that version to the new boot location.* 3. Click **Activate**. Device B reboots to the new software image boot location in offline state.

Option	Description
	Note: *If the device appears to be taking a long time to reboot, do not cycle the power off and on. Instead, verify the status of the device by connecting to its serial console port. The device might be performing firmware upgrades.*
Reboot from version 11.4.0, or later	**1.** On the Main menu, click **System** > **Software Management** > **Boot Locations**. **2.** In the Boot Location list, click the boot location of the installed new software image. **3.** From the **Install Configuration** list, select **Yes**. The **Source Volume** list appears. **4.** From the **Source Volume** list, select the location of the configuration to install when activating the boot location of the new software image. For example, for an installation of a new software image on HD1.3, selecting **HD1.2:11.6.0** installs a version 11.6.0 configuration. **5.** Click **Activate**. Device B reboots to the new software image boot location in offline state. ***Note:*** *If the device appears to be taking a long time to reboot, do not cycle the power off and on. Instead, verify the status of the device by connecting to its serial console port. The device might be performing firmware upgrades.*

5. If the BIG-IP system is configured to use a network HSM, reinstall and configure the HSM client software.

   Important: *You must reinstall network HSM client software on this device before upgrading another device in the device group, to ensure that traffic groups using the network HSM function properly.*

6. Release Device B from offline state.
   a) On the Main menu, click **Device Management** > **Devices**.
   b) Click the name of Device B.
   The device properties screen opens.
   c) Click **Release Offline**.
   Device B changes to standby state.

The new version of BIG-IP software is installed on Device B with configured traffic groups in standby state.

Upgrading the Device C system

The following prerequisites apply in upgrading Device C.

- Device C must be prepared to upgrade the software to new version software.
- Either the latest hotfix image file, if available, or the new version software image file is downloaded and accessible.

  Important: *If you want to upgrade to a BIG-IP® system hotfix image file that applies to incremental major version software, you must install the incremental version software before installing the hotfix image file. For example, if you want to upgrade from BIG-IP version 11.x software to a 12.x hotfix image file, then you must install a version 12.x software image file before you install the hotfix image file.*

- If the BIG-IP system is configured to use a network hardware security module (HSM), you must reinstall network HSM client software on Device B before upgrading Device C, to ensure that traffic groups using the network HSM function properly.
- Device C is in active state.

After you prepare Device C for upgrading the software, you force the device offline, reactivate the software license, and install the new version software.

1. Force Device C to offline state.
   a) On the Main menu, click **Device Management** > **Devices**.
   b) Click the name of Device C.
   The device properties screen opens.
   c) Click **Force Offline**.

   Device C changes to offline state.

   Important: *Once Device C changes to offline state, ensure that the other devices pass traffic normally for all active traffic groups.*

   Note: *When* ***Force Offline*** *is enabled, make sure to manage the system using the management port or console. Connections to self IP addresses are terminated when* ***Force Offline*** *is enabled.*

   ---
2. Reactivate the software license.
   a) On the Main menu, click **System** > **License**.
   b) Click **Re-activate**.
   c) For the **Activation Method** setting, select the **Automatic (requires outbound connectivity)** option.
   d) Click **Next**.
   The BIG-IP software license renews automatically.
   e) Click **Continue**.
3. Install either the latest hotfix image, if available, or the new version software.

   Important: *If you want to upgrade to a BIG-IP system hotfix image file that applies to incremental major version software, you must install the incremental version software before installing the hotfix image file. For example, if you want to upgrade from BIG-IP version 11.x software to a 12.x hotfix image file, then you must install a version 12.x software image file before you install the hotfix image file.*

Option	Description
Install the latest hotfix image	**1.** On the Main menu, click **System** > **Software Management** > **Hotfix List**. **2.** In the Available Images area, select the check box for the hotfix image, and click **Install**. The Install Software Hotfix popup screen opens. **3.** From the **Volume set name** list, select the location of the new version software volume to install the hotfix image, and click **Install**. ***Important:*** *In the* ***Install Status*** *list for the specified location, a progress bar indicates the status of the installation. Ensure that installation successfully completes, as indicated by the progress bar, before proceeding.* ***Note:*** *The format for a volume set name is lower case only, alphanumeric with hyphenation, and limited to 32 characters.*
Install the new version software	**1.** On the Main menu, click **System** > **Software Management** > **Image List**. **2.** In the Available Images area, select the check box for the new version software image, and click **Install**. The Install Software Image popup screen opens.

Option	Description
	3. From the **Volume set name** list, select a location to install the image, and click **Install**. ***Important:*** *In the* ***Install Status*** *list for the specified location, a progress bar indicates the status of the installation. Ensure that installation successfully completes, as indicated by the progress bar, before proceeding.* ***Note:*** *The format for a volume set name is lower case only, alphanumeric with hyphenation, and limited to 32 characters.*

4. Reboot Device C to the location of the installed new software image.

Note: *When upgrading a device group from version 11.x, or later, software to the latest version software, mirroring does not function until all devices in the device group complete rebooting to the latest version. F5 Networks® recommends upgrading software during a scheduled maintenance window, to minimize traffic disruption when devices run different software versions.*

Option	Description
Reboot from version 11.3.0, or earlier	1. On the Main menu, click **System** > **Software Management** > **Boot Locations**. 2. In the Boot Location list, click the boot location of the installed new software image. ***Note:*** *Upgrading from version 11.3.0, or earlier, automatically installs the configuration of that version to the new boot location.* 3. Click **Activate**. Device C reboots to the new software image boot location in offline state. ***Note:*** *If the device appears to be taking a long time to reboot, do not cycle the power off and on. Instead, verify the status of the device by connecting to its serial console port. The device might be performing firmware upgrades.*
Reboot from version 11.4.0, or later	1. On the Main menu, click **System** > **Software Management** > **Boot Locations**. 2. In the Boot Location list, click the boot location of the installed new software image. 3. From the **Install Configuration** list, select **Yes**. The **Source Volume** list appears. 4. From the **Source Volume** list, select the location of the configuration to install when activating the boot location of the new software image. For example, for an installation of a new software image on HD1.3, selecting **HD1.2:11.6.0** installs a version 11.6.0 configuration. 5. Click **Activate**. Device C reboots to the new software image boot location in offline state. ***Note:*** *If the device appears to be taking a long time to reboot, do not cycle the power off and on. Instead, verify the status of the device by connecting to its serial console port. The device might be performing firmware upgrades.*

5. If the BIG-IP system is configured to use a network hardware security module (HSM), reinstall and configure the HSM client software.

> ***Important:*** *You must reinstall network HSM client software on this device, to ensure that traffic groups using the network HSM function properly.*

6. Release Device C from offline state.
   a) On the Main menu, click **Device Management** > **Devices**.
   b) Click the name of Device C.
   The device properties screen opens.
   c) Click **Release Offline**.
   Device C changes to standby state.
7. On the Main tab, click **Device Management** > **Overview**.
8. In the Devices area of the screen, choose the device that shows a sync status of `Changes Pending`.
9. In the Sync Options area of the screen, select **Push the selected device configuration to the group**.
10. Click **Sync**.

The new version of BIG-IP® software is installed on Device C with configured traffic groups in standby state.

Changing states of the traffic groups

Manually configuring active state traffic groups across devices within a device group involves forcing an active state traffic group on a device to standby state, and retargeting that active state traffic group to a different device. Completing these tasks results in active state traffic groups on the appropriate devices in a device group.

Viewing a list of traffic groups for a device

You can view a list of traffic groups for the device group. Using this list, you can add floating IP addresses to a traffic group, force a traffic group into a Standby state, and view information such as the current and next-active devices for a traffic group and its HA load factor.

1. On the Main tab, click **Device Management** > **Traffic Groups**.
2. In the Name column, view the names of the traffic groups on the local device.

Forcing a traffic group to a standby state

You perform this task when you want the selected traffic group on the local device to fail over to another device (that is, switch to a `Standby` state). Users typically perform this task when no automated method is configured for a traffic group, such as auto-failback or an HA group. By forcing the traffic group into a `Standby` state, the traffic group becomes active on another device in the device group. For device groups with more than two members, you can choose the specific device to which the traffic group fails over.

1. Log in to the device on which the traffic group is currently active.
2. On the Main tab, click **Device Management** > **Traffic Groups**.
3. In the Name column, locate the name of the traffic group that you want to run on the peer device.
4. Select the check box to the left of the traffic group name.

   If the check box is unavailable, the traffic group is not active on the device to which you are currently logged in. Perform this task on the device on which the traffic group is active.
5. Click **Force to Standby**.
   This displays target device options.
6. Choose one of these actions:

- If the device group has two members only, click **Force to Standby**. This displays the list of traffic groups for the device group and causes the local device to appear in the Next Active Device column.
- If the device group has more than two members, then from the **Target Device** list, select a value and click **Force to Standby**.

The selected traffic group is now in a standby state on the local device and active on another device in the device group.

Verifying a BIG-IP device group upgrade

When you have completed upgrading the BIG-IP® device group from version 11.x, or later, to the new version, you should verify that the upgraded configuration is working properly.

1. Verify the Platform configuration for each device.

a) On the Main menu, click **System** > **Platform**.

b) For the **Root Folder Device Group** setting, verify that the device group is identical on each device.

c) From the **Root Folder Traffic Group** list, verify that the correct traffic group (**traffic-group-1**) is selected.

2. Verify the configuration for each device.

a) On the Main menu, click **Device Management** > **Devices**.

b) Verify the following information for the device and the peer devices.

- active-standby status
- device name
- management IP address
- hostname
- TMOS version

c) On the Main menu, click **Device Management** > **Device Trust** > **Peer List**.

d) Verify that the peer devices are specified as Peer Authority Devices.

Note: *Ensure that all information for each peer device appears correctly and completely.*

3. Verify the traffic groups for each device.

a) On the Main menu, click **Device Management** > **Traffic Groups**.

b) From the Name list, click a traffic group.

c) If you configured **MAC Masquerade** addresses for VLANs on the devices, verify that the **traffic-group-1** includes an address in the **MAC Masquerade Address** field.

d) Verify that the floating traffic group is correct.

e) Verify that the failover objects are correct.

4. Verify the Current ConfigSync State for each device.

a) On the Main menu, click **Device Management** > **Overview**.

b) In the Devices area of the screen, in the Sync Status column, verify that each device shows a sync status of green.

Implementation result

Your upgrade of the BIG-IP® device group from version 11.x or 12.x to the new version software is now complete. The new version software configuration includes a device group with three devices (Device A, Device B, and Device C) and three traffic groups (`traffic-group-1`, `traffic-group-2`, and `traffic-group-3`), with a traffic group on each device in active state.

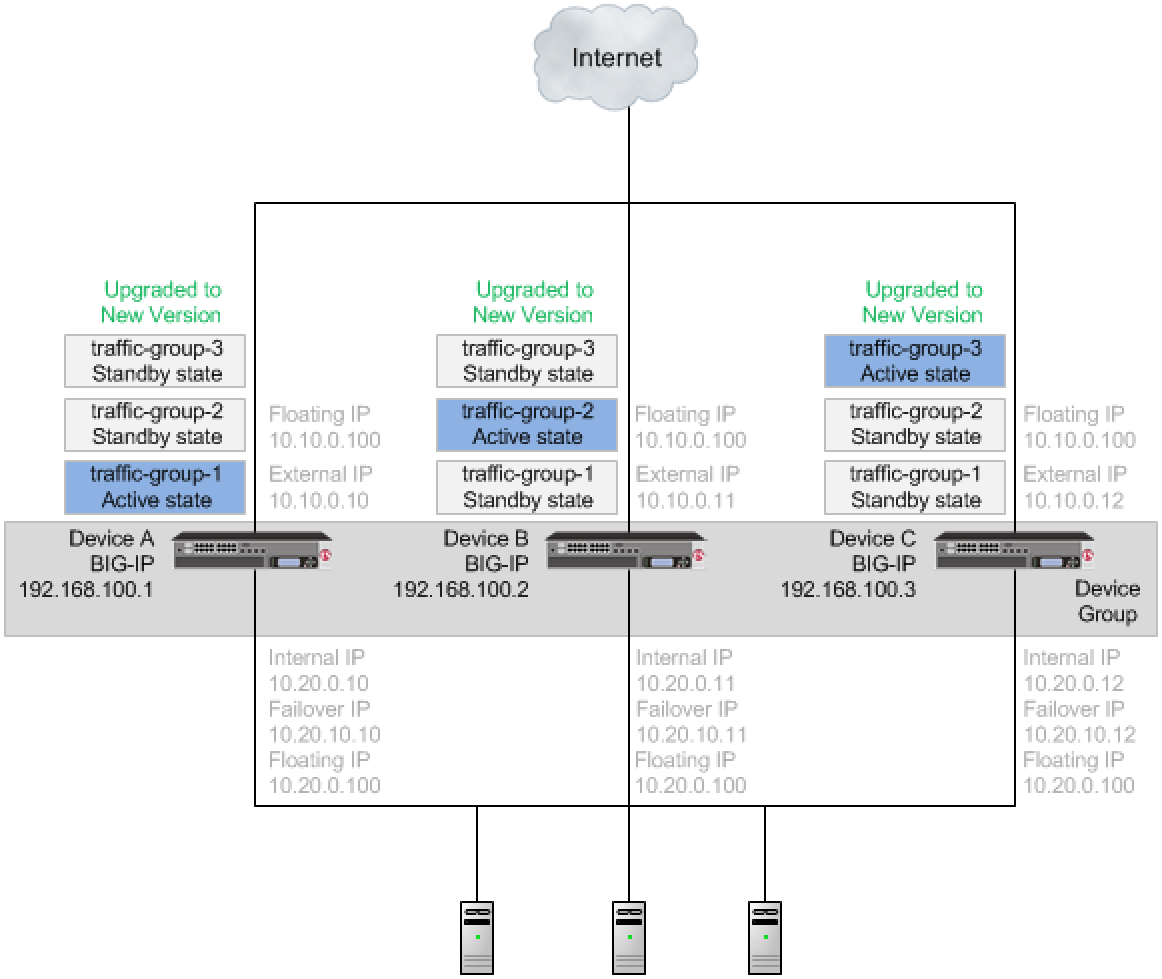

Figure 6: An upgraded device group

Upgrading Version 10.x BIG-IP Active-Standby Systems

Overview: Upgrading BIG-IP active-standby systems

A BIG-IP® system active-standby pair for version 10.x includes one BIG-IP system operating in active mode (Device A) and one BIG-IP system operating in standby mode (Device B).

Important: *In order to upgrade version 10.0.0 or 10.0.1 to the new version software, you must first upgrade to version 10.1.0 or 10.2.x, and then upgrade version 10.1.0 or 10.2.x to the new version software. Additionally, you can only upgrade version 10.1.0 or 10.2.x to version 12.x if you have not provisioned Global Traffic Manager™ (GTM™).*

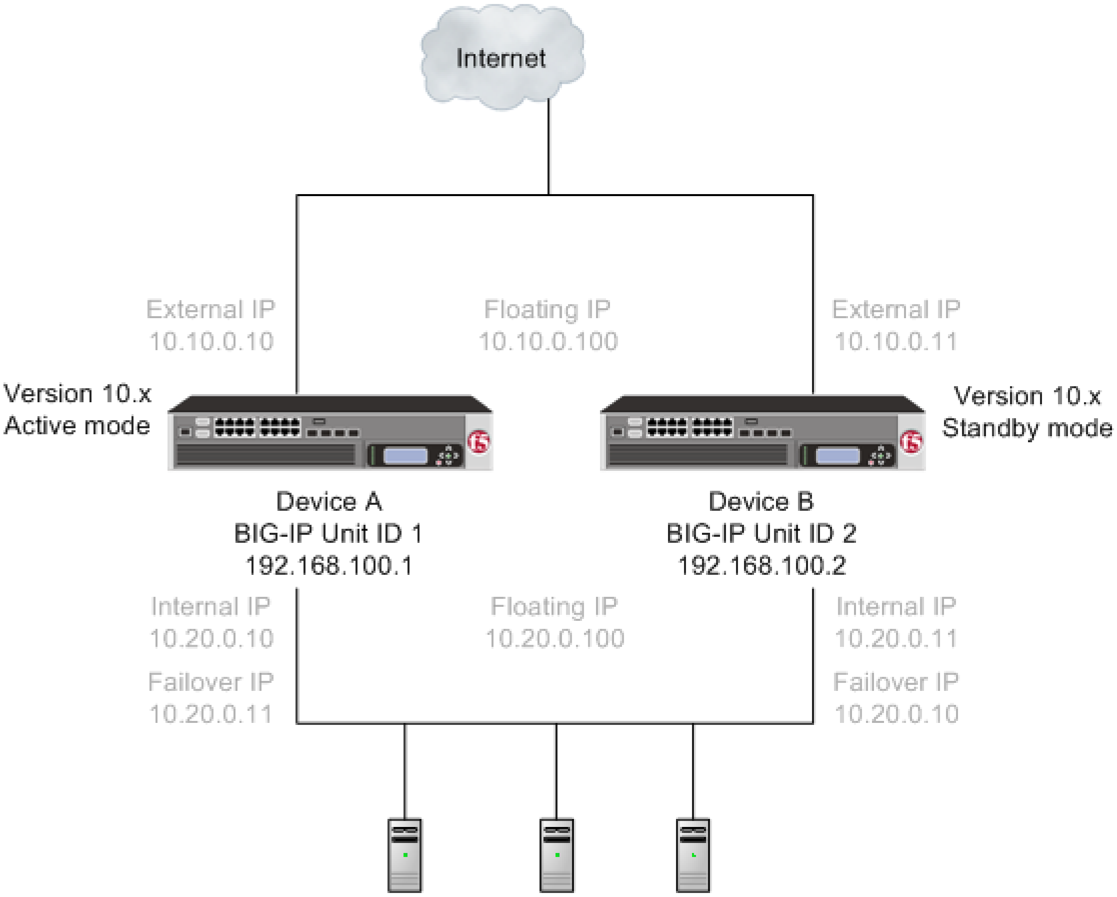

Figure 7: A version 10.x active-standby pair

After preparing the devices for an upgrade to the new version software, you force Device B to offline mode, and then install the new version software onto Device B (the offline device). When you finish the installation of the new version software onto Device B, it creates a traffic group called `traffic-group-1`. The new version software traffic group is in standby state on Device B, and Device A (the version 10.x device) is in active mode. Note that the Unit ID that was used in version 10.x becomes obsolete in the new version software.

Important: *Once Device B reboots, if the BIG-IP system is configured to use a network hardware security module (HSM), you must reinstall network HSM client software on Device B before upgrading Device A, to ensure that traffic groups using the network HSM function properly.*

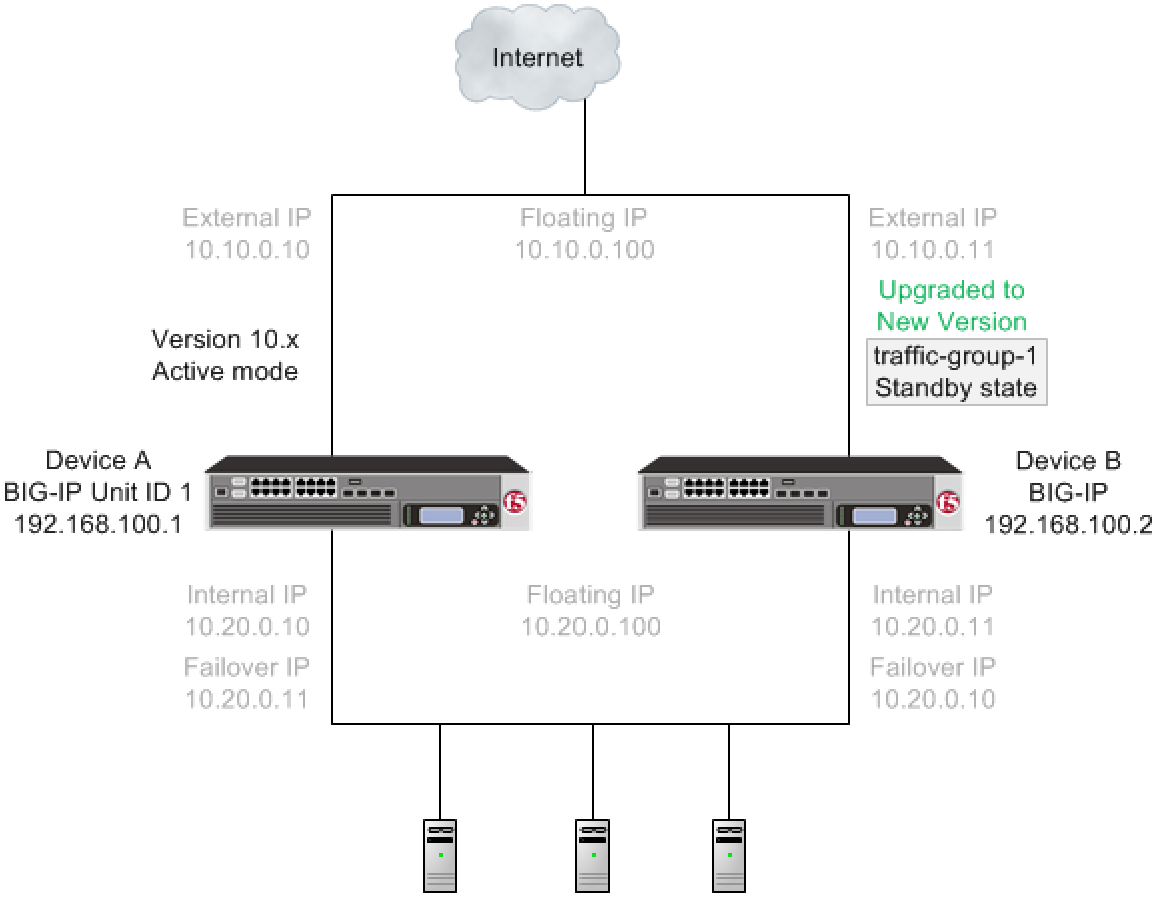

Figure 8: A version 10.x device in active mode and a new software version traffic group in standby state

With the new version software installed on Device B and `traffic-group-1` in standby state, you can force Device A to offline mode, changing Device B to active state so that it can pass traffic, and then install the new software version onto Device A. When installation of the new version software onto Device A completes, you can reboot Device A to the location of the new version software image.

Important: *Once Device A reboots, if the BIG-IP system is configured to use a network HSM, you must reinstall network HSM client software on Device A to ensure that traffic groups using the network HSM function properly.*

When you complete upgrading both devices to the new version software, the BIG-IP configuration includes a traffic group in active state on Device B, a traffic group in standby state on Device A, and a device group that includes both devices.

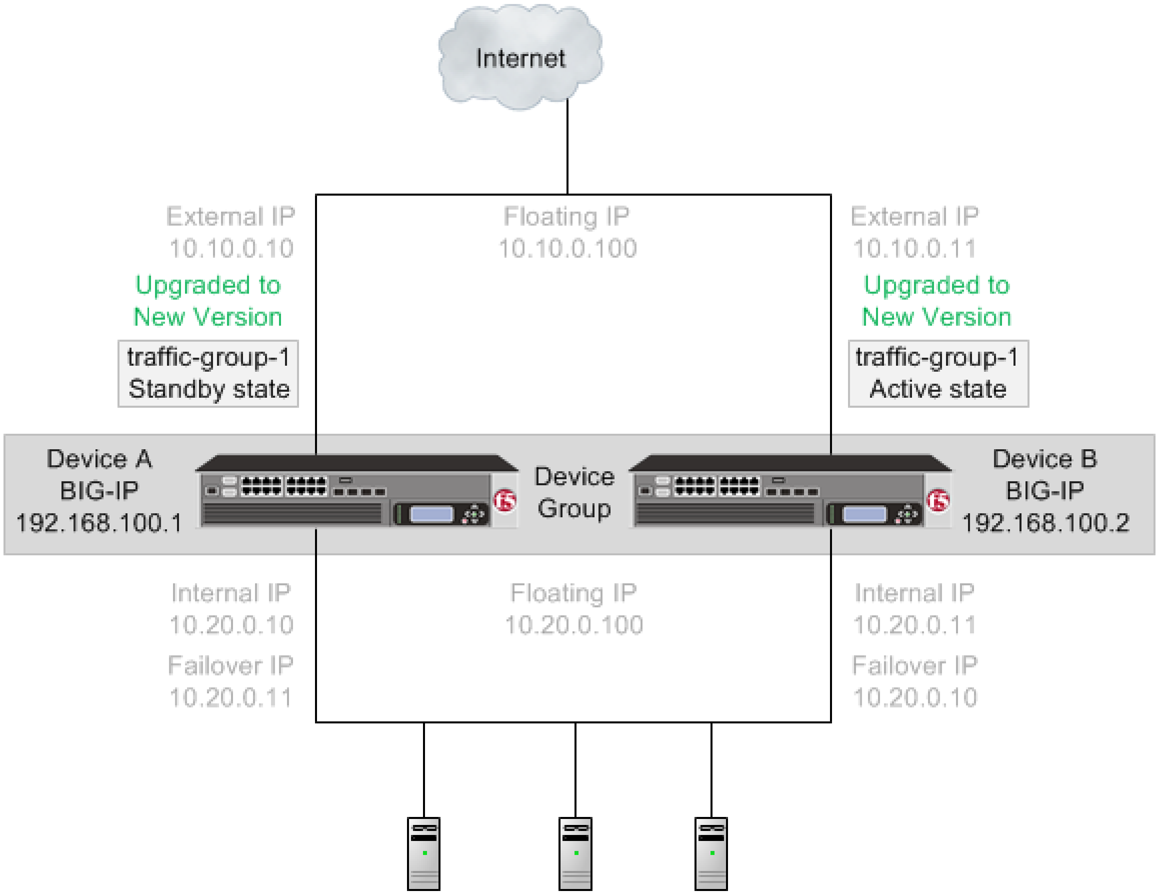

Figure 9: A new version software traffic group in active and standby states

An upgrade of BIG-IP active-standby systems to the new version software involves the following tasks.

Task	Description
Preparing Device A (the active mode BIG-IP 1 system) and Device B (the standby mode BIG-IP 2 system)	In preparing to upgrade the active-standby BIG-IP systems to the new version software, you need to understand any specific configuration or functional changes from the previous version, and prepare the systems. You also download the new version of software from the AskF5 web site (`http://support.f5.com/kb/en-us.html`) and import the files onto each device.
Forcing Device B to offline mode	When you complete preparation of Device B, you can force Device B to offline mode.
Upgrading Device B (the offline mode BIG-IP 2 system)	Once Device B is in offline mode, you can upgrade the software on that device, and then reboot Device B to the location of the new version software image. Device B completes rebooting with `traffic-group-1` in standby state. ***Important:*** *Once Device B reboots, if the BIG-IP system is configured to use a network hardware security module (HSM), you must reinstall network HSM client software on Device B before upgrading*

Task	Description
	Device A, to ensure that traffic groups using the network HSM function properly.
Forcing Device A to offline mode	When Device B completes rebooting to the location of the new version software image, you can force Device A to offline mode, changing `traffic-group-1` on Device B to active state.
Upgrading Device A (the offline mode BIG-IP 1 system)	Once Device A is in offline mode, you can upgrade the software on Device A, and then reboot Device A to the location of the new version software image. When Device A completes rebooting, `traffic-group-1` is in standby state on Device A and in active state on Device B. ***Important:*** *Once Device A reboots, if the BIG-IP system is configured to use a network HSM, you must reinstall network HSM client software on Device A to ensure that traffic groups using the network HSM function properly.*
Verifying the upgrade	Finally, you should verify that your active and standby BIG-IP systems are functioning properly.
Configuring module-specific settings	According to your understanding of the configuration and functional changes from the previous version, you can reconfigure any customized module settings.

DSC components

Device service clustering (DSC®) is based on a few key components.

Devices

A *device* is a physical or virtual BIG-IP® system, as well as a member of a local trust domain and a device group. Each device member has a set of unique identification properties that the BIG-IP system generates. For device groups configured for failover, it is important that the device with the smallest capacity has the capacity to process all traffic groups. This ensures application availability in the event that all but one device in the device group become unavailable for any reason.

Device groups

A *device group* is a collection of BIG-IP devices that trust each other and can synchronize, and sometimes fail over, their BIG-IP configuration data. A *Sync-Failover* device group contains devices that synchronize configuration data and support traffic groups for failover purposes when a device becomes unavailable. The BIG-IP system supports either homogeneous or heterogeneous hardware platforms within a device group.

Important: *BIG-IP module provisioning must be equivalent on all devices within a device group. For example, module provisioning is equivalent when all device group members are provisioned to run BIG-IP® Local Traffic Manager™ (LTM®) and BIG-IP® Application Security Manager™ (ASM™) only. Maintaining equivalent module provisioning on all devices ensures that any device in the device group can process module-specific application traffic in the event of failover from another device.*

Traffic groups

A *traffic group* is a collection of related configuration objects (such as a virtual IP address and a self IP address) that run on a BIG-IP device and process a particular type of application traffic. When a BIG-IP device becomes unavailable, a traffic group can float to another device in a device group to ensure that application traffic continues to be processed with little to no interruption in service.

Device trust and trust domains

Underlying the success of device groups and traffic groups is a feature known as device trust. *Device trust* establishes trust relationships between BIG-IP devices on the network, through mutual certificate-based authentication. A *trust domain* is a collection of BIG-IP devices that trust one another and is a prerequisite for creating a device group for config sync and failover operations. The trust domain is represented by a special system-generated and system-managed device group named `device_trust_group`, which is used to synchronize trust domain information across all devices.

Folders

Folders are containers for the configuration objects on a BIG-IP device. For every administrative partition on the BIG-IP system, there is a high-level folder. At the highest level of the folder hierarchy is a folder named `root`. The BIG-IP system uses folders to affect the level of granularity to which it synchronizes configuration data to other devices in the device group.

About traffic groups

Traffic groups are the core component of failover. A *traffic group* is a collection of related configuration objects, such as a floating self IP address, a floating virtual IP address, and a SNAT translation address, that run on a BIG-IP® device. Together, these objects process a particular type of application traffic on that device.

When a BIG-IP® device goes offline, a traffic group floats (that is, fails over) to another device in the device group to make sure that application traffic continues to be processed with minimal interruption in service.

A traffic group is first active on the device you created it on. If you want an active traffic group to be active on a different device than the one you created it on, you can force the traffic group to switch to a standby state. This causes the traffic group to fail over to (and become active on) another device in the device group. The device it fails over to depends on how you configured the traffic group when you created it.

***Note:** A Sync-Failover device group can support a maximum of 127 floating traffic groups.*

Task summary

The upgrade process involves preparation of the two BIG-IP® devices (Device A and Device B) configured in an active-standby implementation, followed by the installation and verification of the new version software on each device. When you upgrade each device, you perform several tasks. Completing these tasks results in a successful upgrade to the new version software on both BIG-IP devices, with a traffic group configured properly for an active-standby implementation.

***Important:** In order to upgrade version 10.0.0 or 10.0.1 to the new version software, you must first upgrade to version 10.1.0 or 10.2.x, and then upgrade version 10.1.0 or 10.2.x to the new version software. Additionally, you can only upgrade version 10.1.0 or 10.2.x to version 12.x if you have not provisioned Global Traffic Manager™ (GTM™).*

Preparing BIG-IP modules for an upgrade from version 10.x to the new version software
Preparing RAID drives for an upgrade
Preparing BIG-IP active-standby systems for an upgrade

Upgrading the standby BIG-IP 2 system
Upgrading the active BIG-IP 1 system
Verifying a BIG-IP active-standby upgrade

Preparing BIG-IP modules for an upgrade from version 10.x to the new version software

Before you upgrade the BIG-IP® system from version 10.x to the new version software, you might need to manually prepare settings or configurations for specific modules.

Access Policy Manager system preparation

The Access Policy Manager® system does not require specific preparation when upgrading from version 10.x to the new version software. However, additional configuration might be required after completing the upgrade to the new software version.

Supported high availability configuration for Access Policy Manager

Access Policy Manager is supported in an Active-Standby configuration with two BIG-IP® systems only.

Important: *Access Policy Manager is not supported in an Active-Active configuration.*

Post-upgrade activities

When you complete upgrading to the new version software, you should consider the following feature or functionality changes that occur for the Access Policy Manager systems. Depending on your configuration, you might need to perform these changes after you upgrade your systems.

Feature or Functionality	Description
Sessions	All users currently logged in while the upgrade occurs will need to log in again.
Authentication agents and SSO methods	If you have deployments using ActiveSync or Outlook Anywhere, where the domain name is part of the user name, you should enable the **Split domain from username** option in the login page agent if the authentication method used in the access policy requires only the user name for authentication. In the BIG-IP® APM® new version software, authentication agents and SSO methods no longer separates the domain name from the user name internally.
iRule for processing URI	If you have deployments where an iRule is used to perform processing on internal access control URI, for example, `/my.policy`, `/myvpn` or other URIs suc as APM system's login page request, you need to enable the iRule events for internal access control URIs because by default, BIG-IP APM new version software does not raise iRule events for internal access control URIs. However, this can be achieved by adding the following code to the iRule: `when CLIENT_ACCEPTED {`

Feature or Functionality	Description

	`ACCESS::restrict_irule_events disable`
	`}`

OAM support	Manually remove all the OAM server-related configurations and reconfigure OAM on BIG-IP APM new version software. OAM configuration is modified to support various OAM 11G related use cases.
Citrix support functionality	The Citrix iRule is no longer visible to the administrator because it is integrated natively in BIG-IP APM new version software. If you have not modified the iRule, then you must enable the **Citrix Support** setting on the virtual server to use Citrix. If you modified the F5-provided Citrix support iRule and want to use the modified iRule, you need to contact F5 support and work with them to replace natively integrated iRules® with your own version of Citrix-supported iRules®.
Reporting functionality	If you used the `adminreports.pl` script for your logging or reporting purposes, this script is no longer available in BIG-IP APM new version software. You need to migrate to the new and enhanced reporting and logging functionality available as a built-in functionality on the new software version.

Application Security Manager system preparation

The BIG-IP® Application Security Manager™ (ASM™) system does not require specific preparation when upgrading from version 10.x to the new version software. No additional configuration is required after completing the upgrade to the new software version.

What to expect after upgrading a redundant system

If you update two redundant systems that are running as an active-standby pair with BIG-IP Application Security Manager (ASM) and BIG-IP® Local Traffic Manager™ (LTM®) provisioned, the system maintains the active-standby status and automatically creates a Sync-Failover device group and a traffic group containing both systems. The device group is enabled for BIG-IP ASM (because both systems have ASM provisioned).

You can manually push or pull the updates (including BIG-IP LTM and ASM configurations and policies) from one system to the other (**Device Management** > **Overview**, click the name of a device, and choose **Sync Device to Group** or **Sync Group to Device**).

Global Traffic Manager system preparation and configuration

BIG-IP® Global Traffic Manager™ systems require specific preparation tasks and changes to upgrade from version 10.x to the new version software.

Preparation Activities

Before you upgrade Global Traffic Manager systems that are in a synchronization group, from any software version to the new version software, you must install the software on an inactive volume on each device using Live Install. After you upgrade each device, you then switch all devices to the new volume at the same time. This is required because devices in a synchronization group that includes the new version software device, cannot effectively probe each other.

Post-upgrade changes

Important: *In BIG-IP version 12.0, BIG-IP Global Traffic Manager is renamed to BIG-IP DNS. After you upgrade, you will see the new name in the product and documentation.*

The following feature or functionality changes occur after you complete the upgrade process to the new version software:

Feature or Functionality	Description
Assigning a BIG-IP system to probe a server to gather health and performance data	Assigning a single BIG-IP system to probe a server to gather health and performance data, in version 10.x, is replaced by a Prober pool in the new software version.

Link Controller system preparation

The BIG-IP® Link Controller™ (LC™) system does not require specific preparation when upgrading from version 10.x to the new version software. No additional configuration is required after completing the upgrade to the new version software.

Local Traffic Manager system preparation

The BIG-IP® Local Traffic Manager™ (LTM®) system does not require specific preparation when upgrading from version 10.x to the new version software. No additional configuration is required after completing the upgrade to the new version software.

MAC masquerade addresses for VLANs

Note: *If you configured* ***MAC Masquerade*** *addresses for VLANs on the version 10.x devices, one of the addresses will be included automatically in the* ***MAC Masquerade Address*** *field for* ***traffic-group-1*** *during the upgrade.*

HTTP Class profiles

F5 Networks® replaced the HTTP Class profile in BIG-IP® version 11.4.0, and later, with the introduction of the Local Traffic Policies feature. During an upgrade to BIG-IP version 11.4.0, if your configuration contains an HTTP Class profile, the BIG-IP system attempts to migrate the HTTP Class profile to an equivalent local traffic policy. For additional support information regarding the change of HTTP Class profiles to Local Traffic Policies, refer to SOL14409 on www.askf5.com.

WebAccelerator module preparation and configuration

BIG-IP® WebAccelerator modules require specific preparation tasks and changes to upgrade from version 10.x to the new version software.

Preparation activities

Before you upgrade the BIG-IP® WebAccelerator™ modules from version 10.x to an Application Acceleration Manager new software version, you need to prepare the systems, based on your configuration. The following table summarizes the applicable tasks that you need to complete.

Feature or Functionality	Preparation Task
Symmetric deployment	You must reconfigure symmetric WebAccelerator modules as asymmetric systems before you upgrade them from version 10.x to the new version software.
Unpublished policies	You must publish any policies that you want to migrate to the new software version. Only published policies are migrated into the new version software.
Signed policies	Signed policies are not supported in the new version software. If you use signed policies, you must replace them with predefined or user-defined policies before upgrading.
Configuration files	Upgrading from version 10.x to the new version software does not include custom changes to configuration files. After upgrading to the new version software, you need to manually restore any customizations made to your configuration files by using the Configuration utility or Traffic Management Shell (`tmsh`). The following list includes examples of configuration files that might have been customized: • `/config/wa/globalfragment.xml.10.x.0`; in the new software version, all `objtype` entries are provided in `tmsh`. • `/config/wa/pvsystem.conf.10.x.0` • `/config/wa/pvsystem.dtd.10.x.0` • `/config/wa/transforms/common.zip.10.x.0`; the new software version does not include transforms.
Debug Options	`X-PV-Info` response headers in version 10.x are changed to `X-WA-Info` response headers in the new software version. The default setting for **X-WA-Info Headers** is **None** (disabled). To use `X-WA-Info` response headers, you will need to change this setting, and update any associated iRules® or scripts, accordingly.

Post-upgrade activities

When you complete upgrading to the new version software, you should consider the following feature or functionality changes that occur for the Application Acceleration Manager modules. Depending upon your configuration, you might need to perform these changes after you upgrade the systems.

Feature or Functionality	Description
Web acceleration	Web acceleration functionality requires configuration of the Web Acceleration profile. ***Important:*** *You must enable an Application Acceleration Manager module application in the*

Feature or Functionality	Description
	Web Acceleration profile to enable the Application Acceleration Manager module.
Compression	Compression functionality requires configuration of the HTTP Compression profile in the new version software.
Request logging	Request logging does not migrate to the new version software. You must recreate the configuration after upgrading by using the Request Logging profile.
Policy logging	Policy logging does not migrate to the new version software. You must recreate the configuration after upgrading by using the Request Logging profile.
URL normalization	URL normalization is not supported in the new version software.
ESI functionality	Edge Side Include (ESI) functionality in the Application Acceleration Manager module is not supported in the new version software, with the exception of ESI invalidations.
iControl® backward compatibility	Backward compatibility for iControl Compression and RAM Cache API settings in the HTTP profile is not supported in the new version software. These settings appear in the HTTP Compression and Web Acceleration profiles in the new software version.

WAN Optimization Manager preparation

BIG-IP® WAN Optimization Manager™ (WOM®) systems do not require specific preparation when upgrading from version 10.x to the new version software. However, in a redundant system configuration, you must upgrade the standby system first (to avoid interrupting traffic on the active system), and then upgrade the other system. No additional configuration is required after completing the upgrade to the new version software.

Preparing RAID drives for an upgrade

If your configuration includes redundant array of independent disks (RAID) drives, you need to verify that the RAID drives are ready for upgrading. If a RAID drive shows errors before upgrading, you will want to contact F5 customer support to resolve the errors before initiating the upgrade.

1. Open the Traffic Management Shell (tmsh).
   `tmsh`
   This starts `tmsh` in interactive shell mode and displays the `tmsh` prompt: `(tmos)#`.
2. Verify the health of RAID disks, ensuring that the drives are not failed or undefined.

   `(tmos)# show sys raid`

```
Sys::Raid::Array: MD1
--------------------
Size (MB) 305245
```

```
Sys::Raid::ArrayMembers
Bay ID Serial Number Name Array Member Array Status
---------------------------------------------------------
1 WD-WCAT18586780 HD2 yes failed
2 WD-WCAT1E733419 HD1 yes ok
```

In this example, the array is labeled MD1 and disk HD2 indicates an error.

3. Verify `Current_Pending_Sector` data displays a `RAW_VALUE` entry of less than `1` on RAID systems.

Option	Description
For version 11.4.0, and later	Run the platform check utility: `(tmos)# run util platform_check`
For version 11.3.x, and earlier	At the command line, run the smartctl utility: `smartctl -t long -d ata /dev/<sda|sdb|hda|hdc>`

```
197 Current_Pending_Sector  0x0032  200  200  000  Old_age  Always  -  0
```

In this example, the `RAW_VALUE` entry is `0`.

4. Verify that no known issues appear in the following log files.
   - Check `/var/log/user.log` for LBA messages indicating failure to recover, for example, `recovery of LBA:226300793 not complete`.
   - Check `/var/log/kern.log` for ATA error entries.

The health of all RAID drives is assessed, enabling you to resolve any issues before proceeding with the BIG-IP® software upgrade.

Preparing BIG-IP active-standby systems for an upgrade

The following prerequisites apply when you upgrade BIG-IP® active and standby devices from version 10.x to the new version software.

- The BIG-IP systems (Device A and Device B) are configured as an active-standby pair.
- Each BIG-IP device is running the same version of 10.x software.
- The BIG-IP active-standby devices are the same model of hardware.

When you upgrade a BIG-IP active-standby pair from version 10.x to the new version software, you begin by preparing the devices.

***Note:** If you prefer to closely observe the upgrade of each device, you can optionally connect to the serial console port of the device that you are upgrading.*

1. For each device, complete the following steps to prepare the configuration and settings.
   a) Examine the Release Notes for specific configuration requirements, and reconfigure the systems, as necessary.

      For example, you must reconfigure version 10.x symmetric BIG-IP® WebAccelerator™ modules as asymmetric systems before upgrading to the new version software.
   b) Examine the Release Notes for specific changes to settings that occur when upgrading from version 10.x to the new version software, and complete any in-process settings.

      For example, you must publish any unpublished WebAccelerator module policies in order for them to migrate to the new software version.
2. From the device that is running the latest configuration, synchronize the configuration to the peer unit.
   a) On the Main menu, click **System** > **High Availability** > **ConfigSync**.

A message appears for the Status Message.

b) Click **Synchronize TO Peer**.

3. For each device, click **System** > **High Availability** > **Redundancy**, and, from the **Redundancy State Preference** list, select **None**.
4. For each device, create a backup file.

a) Access the `tmsh` command line utility.

b) At the prompt, type `save /sys ucs /shared/filename.ucs`.

c) Copy the backup file to a safe location on your network.

***Note:** For additional support information about backing up and restoring BIG-IP system configuration files, refer to SOL11318 on `www.askf5.com`.*

5. Download the BIG-IP new version software `.iso` file, and, if available, the latest hotfix `.iso` file from the AskF5™ downloads web site (`https://downloads.f5.com`) to a preferred location.
6. Import either the latest BIG-IP hotfix image file, if available, or the new version software upgrade image file to each device.

Option	Description
Import the latest BIG-IP system hotfix image and SIG file	**1.** On the Main menu, click **System** > **Software Management** > **Hotfix List** > **Import**. **2.** Click **Browse**, locate and click the SIG file (Hotfix-BIGIP-hf-xx.x.x.x.x.xxxx.HFx.iso.384.sig), click **Open**, and click **Import**. **3.** Click **Browse**, locate and click the image file, click **Open**, and click **Import**. **4.** When the hotfix image file completes uploading to the BIG-IP device, click **OK**. A link to the image file appears in the Software Image list.
Import the new version software image and SIG file	**1.** On the Main menu, click **System** > **Software Management** > **Image List** > **Import**. **2.** Click **Browse**, locate and click the SIG file (BIGIP-13.x.x.x.x.xxxx.iso.384.sig), click **Open**, and click **Import**. **3.** Click **Browse**, locate and click the upgrade image file, click **Open**, and click **Import**. ***Note:** BIG-IP version 13.x, and later, provides upgrade and recovery image files. An upgrade image file (for example, BIGIP-13.x.x.x.x.xxx.iso) omits End User Diagnostics (EUD) software, which includes tests that report on hardware components. A recovery image file (for example, BIGIP-RECOVERY-13.x.x.x.x.xxx.iso) includes EUD software.* **4.** When the software image file completes uploading to the BIG-IP device, click **OK**. A link to the image file appears in the Software Image list.

7. (Optional) Verify the integrity of the imported software image file.

Option	Description
Use SIG verification (recommended)	**1.** At the command line, determine the filename of the applicable public key file. Example: `# ls /usr/lib/install/archive.pubkey*pem`. The list of `archive.pubkey` files appears. **2.** Using the openssl utility, verify the integrity of the imported software image file.

Option	Description
	Example: `# openssl dgst -sha384 -verify usr/lib/install/archive.pubkey.xxxxxxxxx.pem -signature shared/images/BIGIP-13.x.x.x.x.xxxx.iso.384.sig shared/images/BIGIP-13.x.x.x.x.xxxx.iso` **Note:** *You must use openssl version 1.0.0, or later. Type* `openssl version` *at the command line to determine the version.* The openssl utility verifies the integrity of the software image file and displays the results. # openssl dgst -sha384 -verify usr/lib/install/archive.pubkey.xxxxxxxxx.pem -signature shared/images/BIGIP-13.x.x.x.x.xxxx.iso.384.sig shared/images/BIGIP-13.x.x.x.x.xxxx.iso Verified OK
Use an MD5 checksum	• Using a tool or utility that computes an md5 checksum, you can verify the integrity of the BIG-IP system latest hotfix `.iso` file or new version `.iso` file.

The BIG-IP devices are prepared to install the latest hotfix or new version software onto Device B (the standby BIG-IP 2 device).

Upgrading the standby BIG-IP 2 system

The following prerequisites apply for this task.

- Device A (the active BIG-IP® 1 system) and Device B (the standby BIG-IP 2 system) must be prepared to upgrade Device B with the new software version software.
- Either the latest hotfix image file, if available, or the new version software image file is downloaded and accessible.

After you prepare Device A (the active BIG-IP 1 system) and Device B (the standby BIG-IP 2 system) for upgrading the software, you force Device B offline, reactivate the software license, and install the new version software onto Device B.

1. Force Device B to offline mode.
   a) On the Main menu, click **System** > **High Availability** > **Redundancy**.
   b) Click **Force Offline**.
   The BIG-IP device (Device B) changes to offline mode.
2. Reactivate the software license.
   a) On the Main menu, click **System** > **License**.
   b) Click **Re-activate**.
   c) For the **Activation Method** setting, select the **Automatic** (requires outbound connectivity) option.
   d) Click **Next**.

   The BIG-IP software license renews automatically.

   e) Click **Continue**.
3. Install either the latest hotfix image, if available, or the new software version.

Option	Description
Install the latest hotfix image	1. On the Main menu, click **System** > **Software Management** > **Hotfix List**. 2. In the Available Images area, select the check box for the hotfix image, and click **Install**. The Install Software Hotfix popup screen opens. 3. From the **Volume set name** list, select the location of the new version software volume to install the hotfix image, and click **Install**. *__Important:__ In the __Install Status__ list for the specified location, a progress bar indicates the status of the installation. Ensure that installation successfully completes, as indicated by the progress bar, before proceeding.*
Install the new version software	1. On the Main menu, click **System** > **Software Management** > **Image List**. 2. In the Available Images area, select the check box for the new software version image, and click **Install**. The Install Software Image popup screen opens. 3. From the **Volume set name** list, select a location to install the image, and click **Install**. *__Important:__ In the __Install Status__ list for the specified location, a progress bar indicates the status of the installation. Ensure that installation successfully completes, as indicated by the progress bar, before proceeding.*

4. Reboot the device to the location of the installed new version software software image.

   __Important:__ Once Device B reboots, if the BIG-IP system is configured to use a network hardware security module (HSM), you must reinstall network HSM client software on Device B before upgrading Device A, to ensure that traffic groups using the network HSM function properly.

   a) On the Main menu, click **System** > **Software Management** > **Boot Locations**.
   b) In the **Boot Location** list, click the boot location of the installed new version software software image.
   c) Click **Activate**.

      The BIG-IP device reboots to the new version software boot location with `traffic-group-1` in standby state.

      __Note:__ If the device appears to be taking a long time to reboot, do not cycle the power off and on. Instead, verify the status of the device by connecting to its serial console port. The device might be performing firmware upgrades.

The new version software is installed on Device B, with `traffic-group-1` in standby state.

Upgrading the active BIG-IP 1 system

The following prerequisites apply in upgrading Device A (the BIG-IP® 1 system).

- Device A (the version 10.x BIG-IP 1 system) must be prepared to upgrade to the new version software.
- Device A is in active mode.
- Device B (the the new version software BIG-IP device with traffic-group-1) is in standby state.
- The new version software image file is downloaded and available.
- If available, the latest hotfix image file is downloaded and available.

After you prepare Device A (the standby BIG-IP 1 system) for upgrading the software, you can perform these steps to upgrade to the new version software.

1. Force Device A to offline mode.

   a) On the Main menu, click **System** > **High Availability** > **Redundancy**.

   b) Click **Force Offline**.

   The BIG-IP device (Device A) changes to offline mode and the peer BIG-IP device (Device B) changes to active state.

   Important: *Once the peer BIG-IP device (Device B) changes to active state, ensure that it passes traffic normally.*

2. Reactivate the software license.

   a) On the Main menu, click **System** > **License**.

   b) Click **Re-activate**.

   c) For the **Activation Method** setting, select the **Automatic (requires outbound connectivity)** option.

   d) Click **Next**.

   The BIG-IP software license renews automatically.

   e) Click **Continue**.

3. Install either the latest hotfix image, if available, or the new version software.

Option	Description
Install the latest hotfix image	**1.** On the Main menu, click **System** > **Software Management** > **Hotfix List**. **2.** In the Available Images area, select the check box for the hotfix image, and click **Install**. The Install Software Hotfix popup screen opens. **3.** From the **Volume set name** list, select the location of the new version software volume to install the hotfix image, and click **Install**. ***Important:*** *In the* ***Install Status*** *list for the specified location, a progress bar indicates the status of the installation. Ensure that installation successfully completes, as indicated by the progress bar, before proceeding.*
Install the new version software	**1.** On the Main menu, click **System** > **Software Management** > **Image List**. **2.** In the Available Images area, select the check box for the new version software image, and click **Install**. The Install Software Image popup screen opens. **3.** From the **Volume set name** list, select a location to install the image, and click **Install**. ***Important:*** *In the* ***Install Status*** *list for the specified location, a progress bar indicates the status of the installation. Ensure that installation successfully completes, as indicated by the progress bar, before proceeding.*

4. Reboot the BIG-IP device (Device A) to the location of the installed new version software image.

   a) On the Main menu, click **System** > **Software Management** > **Boot Locations**.

   b) In the **Boot Location** list, click the boot location of the installed the new version software image.

   c) Click **Activate**.

   The BIG-IP device (Device A) reboots to the new version software boot location with traffic-group-1 in standby state.

   Note: *If the device appears to be taking a long time to reboot, do not cycle the power off and on. Instead, verify the status of the device by connecting to its serial console port. The device might be performing firmware upgrades.*

5. On the Main tab, click **Device Management** > **Overview**.
6. In the Devices area of the screen, choose the device that shows a sync status of `Changes Pending`.
7. In the Sync Options area of the screen, select **Push the selected device configuration to the group**.
8. Click **Sync**.

The new version software is installed on Device A (the BIG-IP system with traffic-group-1 in standby state).

Verifying a BIG-IP active-standby upgrade

When you have completed upgrading the BIG-IP active-standby pair from version 10.x to the new version software, you should verify that the upgraded configuration is working properly. Perform the following steps to verify the new version software upgrade.

1. Verify the Platform configuration for each device.
   a) On the Main menu, click **System** > **Platform**.
   b) For the **Root Folder Device Group** setting, verify that the device group is identical on the pair of devices.
   c) From the **Root Folder Group** list, verify that the correct traffic group (**traffic-group-1**) is selected.
2. Verify the configuration for each device.
   a) On the Main menu, click **Device Management** > **Devices**.
   b) Verify the following information for the device and the peer device.

      - active-standby status
      - device name
      - management IP address
      - hostname
      - TMOS version

   c) On the Main menu, click **Device Management** > **Device Trust** > **Peer List**.
   d) Verify that the peer device is specified as a Peer Authority Device.

      Note: *Ensure that all information for the peer device appears correctly and complete.*
3. Verify the traffic groups for each device.
   a) On the Main menu, click **Device Management** > **Traffic Groups**.
   b) Click **traffic-group-1**.
   c) If you configured **MAC Masquerade** addresses for VLANs on the version 10.x devices, verify that the **traffic-group-1** includes an address in the **MAC Masquerade Address** field.
   d) Verify that the floating traffic group is correct.
   e) Verify that the failover objects are correct.
4. Verify the Current ConfigSync State for each device.
   a) On the Main menu, click **Device Management** > **Overview**.
   b) In the Devices area of the screen, in the Sync Status column, verify that each device shows a sync status of green.

Implementation result

Your upgrade of the BIG-IP® active-standby pair from version 10.x to the new version software is now complete. The new version software configuration includes a device group with two devices (Device A and Device B) and a traffic group (`traffic-group-1`), with the traffic group on one device (Device B) in active state and the traffic group on the other device (Device A) in standby state.

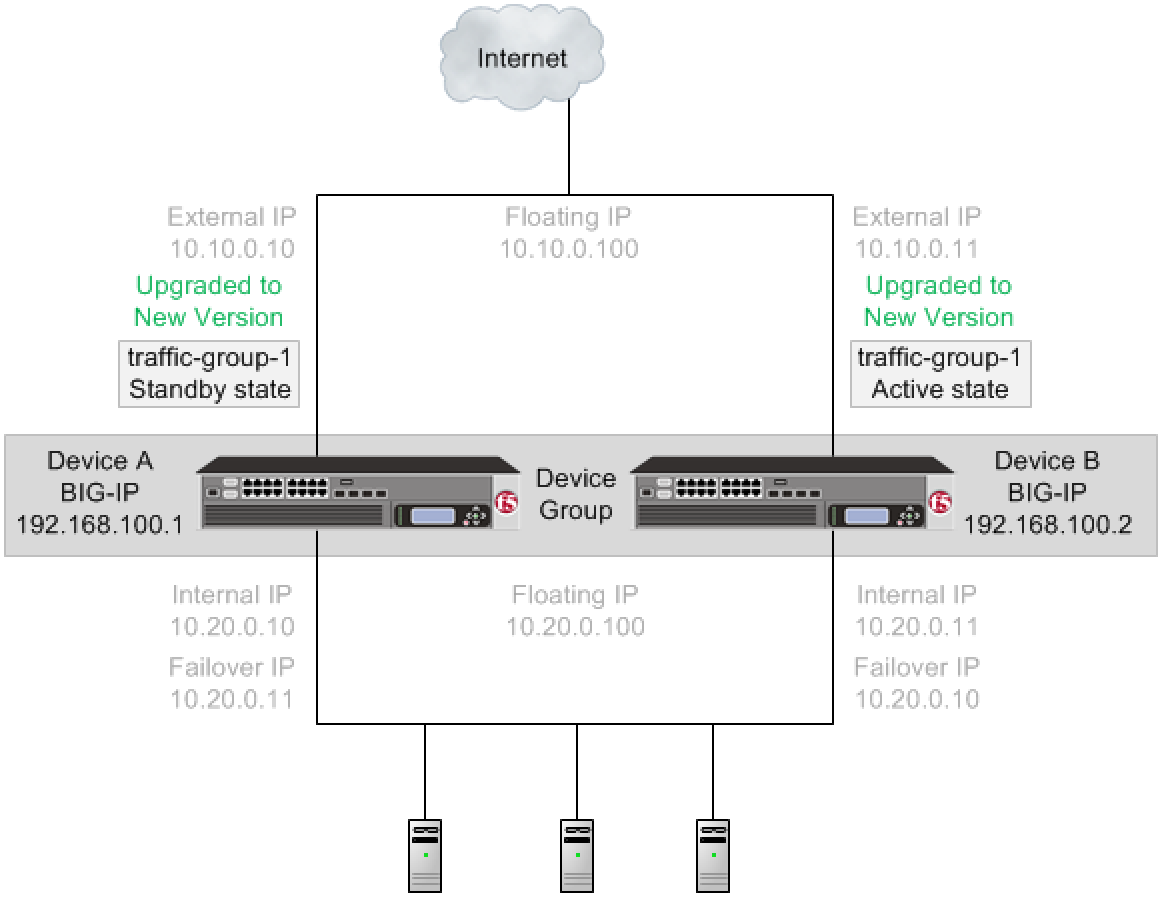

Figure 10: A new version software device group and traffic group

Upgrading Version 10.x BIG-IP Active-Active Systems

Overview: Upgrading BIG-IP active-active systems

A BIG-IP® system active-active pair for version 10.x includes two BIG-IP systems operating in active mode (Device A and Device B).

Important: *In order to upgrade version 10.0.0 or 10.0.1 to the new version software, you must first upgrade to version 10.1.0 or 10.2.x, and then upgrade version 10.1.0 or 10.2.x to the new version software. Additionally, you can only upgrade version 10.1.0 or 10.2.x to version 12.x if you have not provisioned Global Traffic Manager™ (GTM™).*

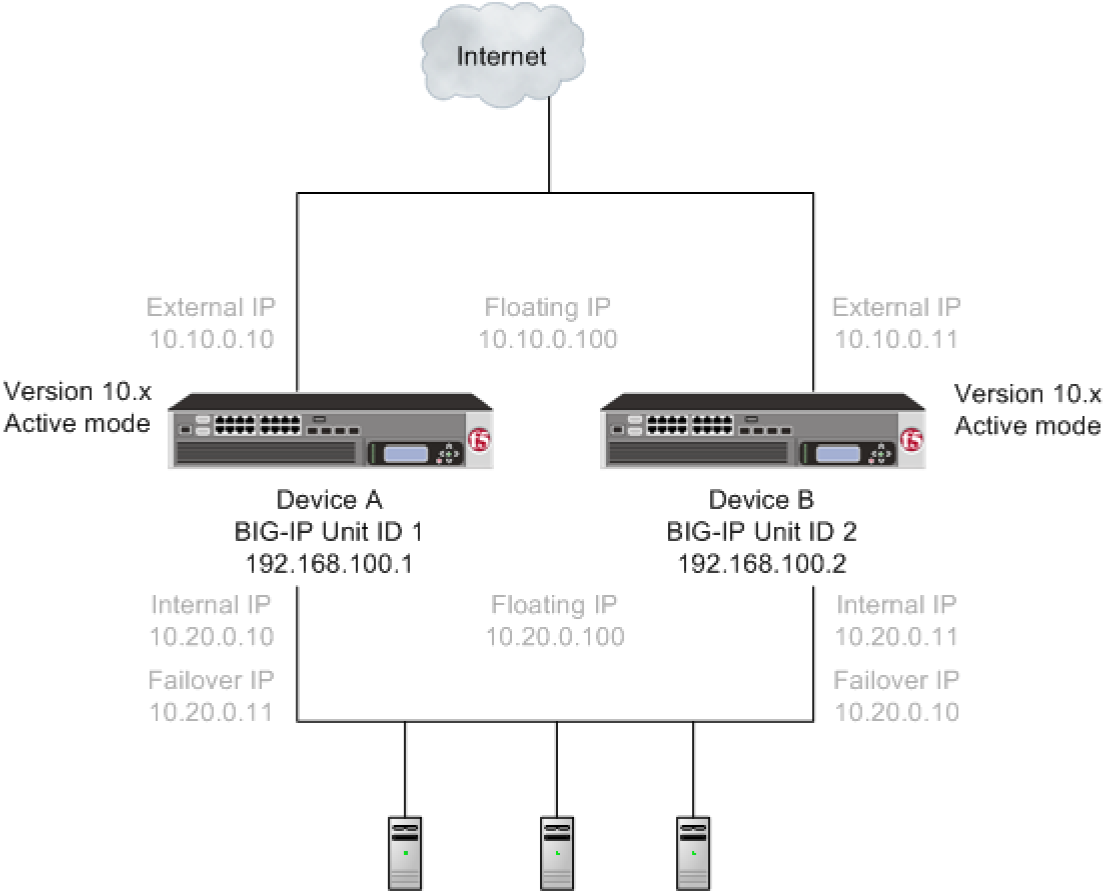

Figure 11: A version 10.x active-active pair

After preparing the devices for an upgrade to the new version software, you force Device B to offline mode, and then install the new version software onto Device B (the offline device).

Important: *Once Device B reboots, if the BIG-IP system is configured to use a network hardware security module (HSM), you must reinstall network HSM client software on Device B before upgrading Device A, to ensure that traffic groups using the network HSM function properly.*

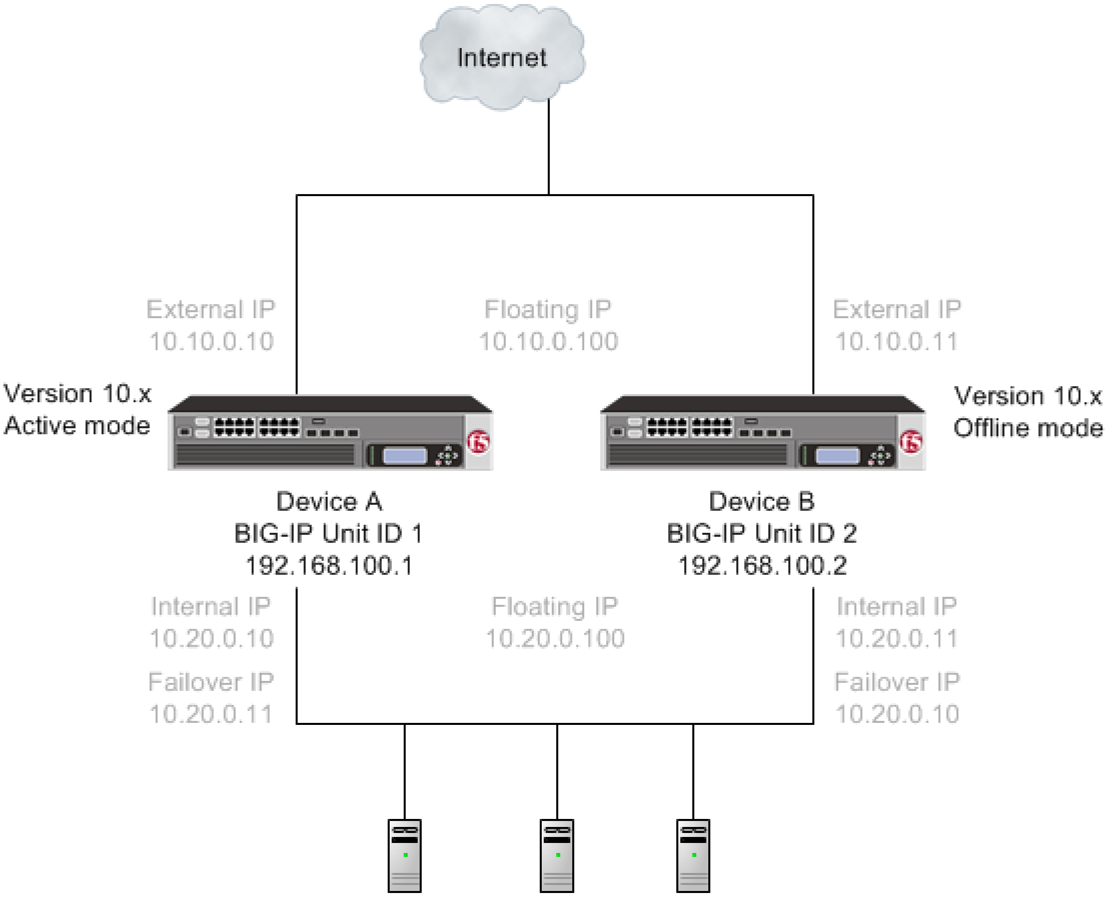

Figure 12: A version 10.x active-offline pair

When you finish the installation of the new version software onto Device B, it creates two traffic groups called `traffic-group-1` and `traffic-group-2`. Each traffic group is in standby state on Device B, and Device A (the version 10.x device) is in active mode. You can then force Device A to offline mode, changing both the new version software traffic groups to active state on Device B. Note that the Unit ID that was used in version 10.x becomes obsolete in the new version software.

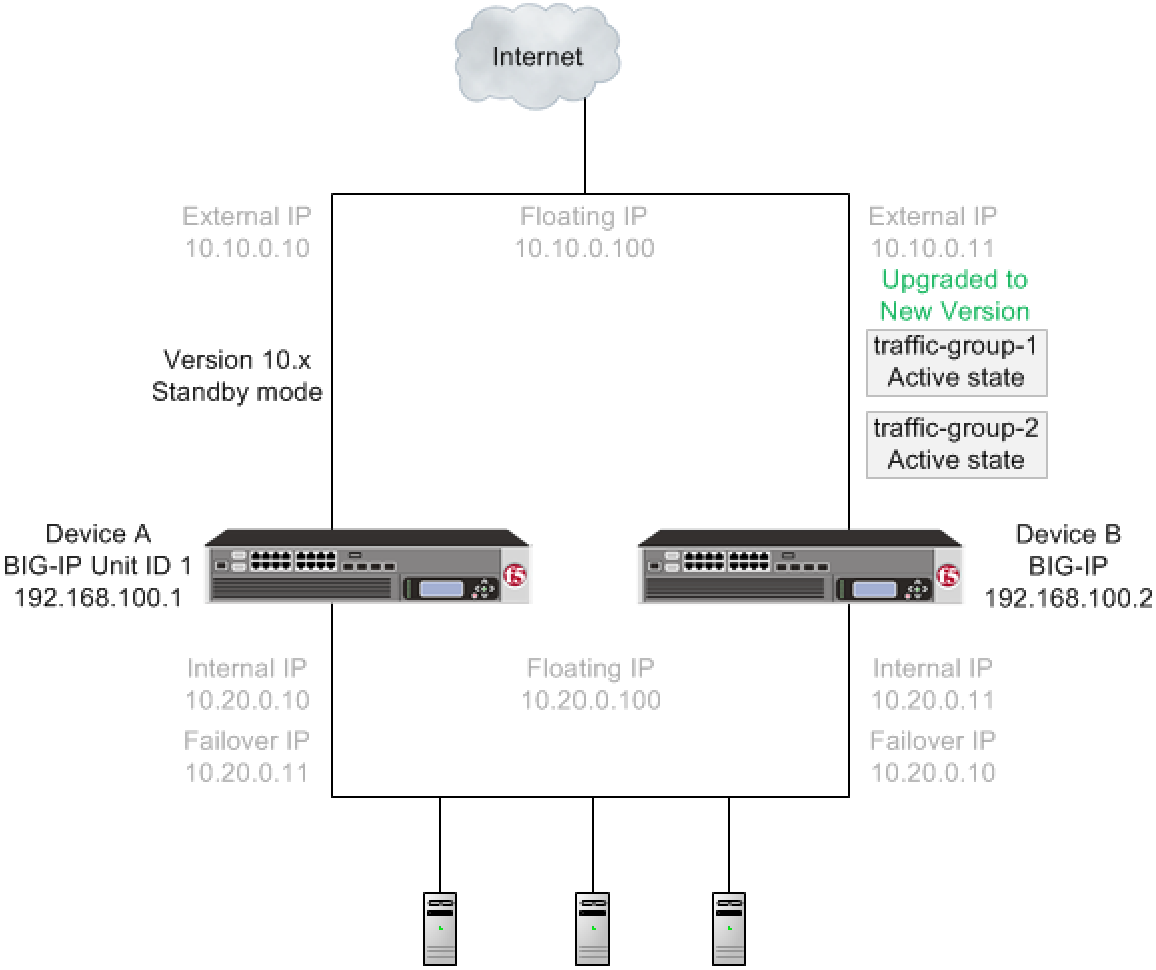

Figure 13: A version 10.x device in offline mode and the new version software traffic groups in active state

You then install the new version software onto Device A.

Important: *Once Device A reboots, if the BIG-IP system is configured to use a network HSM, you must reinstall network HSM client software on Device A to ensure that traffic groups using the network HSM function properly.*

When you complete upgrading both devices to the new version software, the BIG-IP system configuration includes `traffic-group-1` and `traffic-group-2` in active state on Device B, a `traffic-group-1` and `traffic-group-2` in standby state on Device A, and a device group that includes both devices.

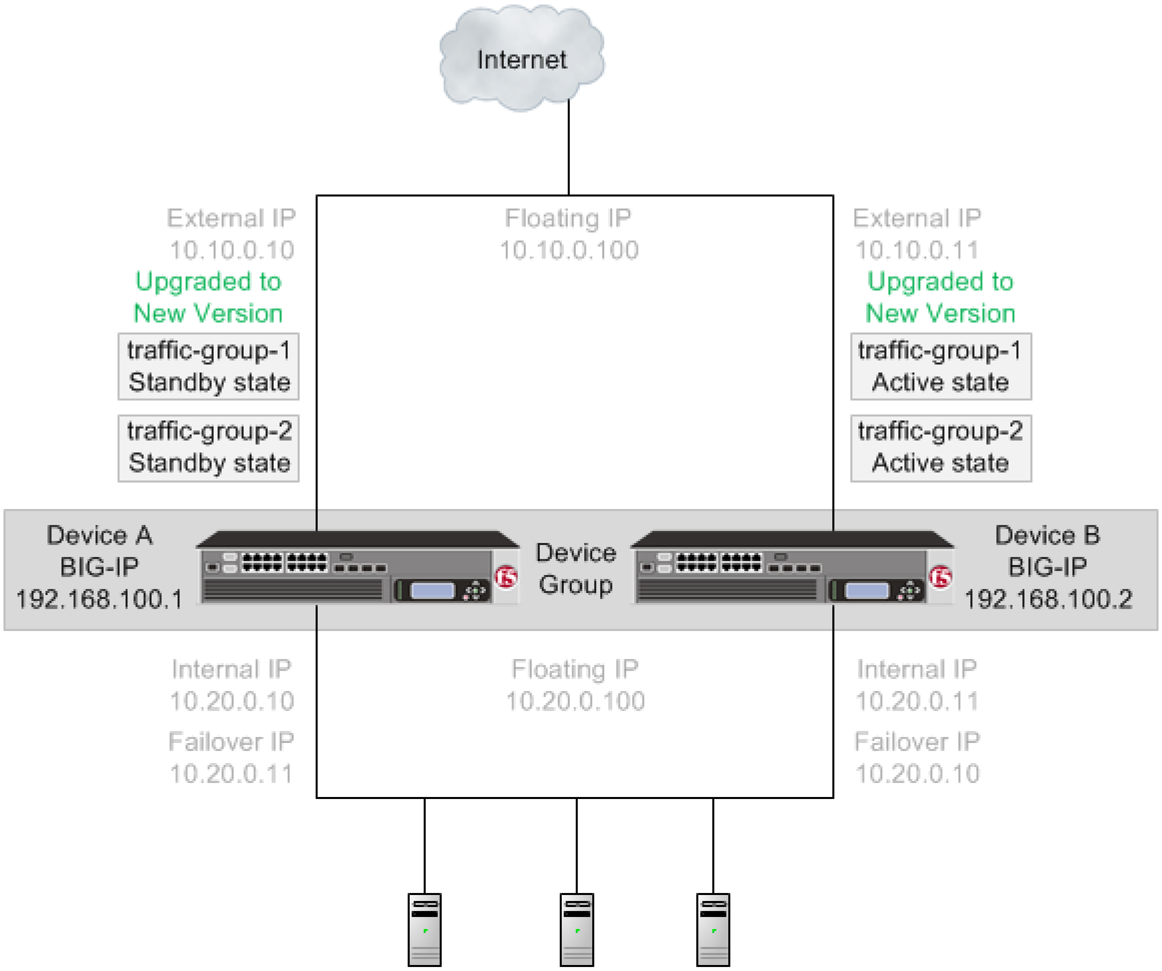

Figure 14: The new version software traffic groups in active state on an upgraded device

Once each device is upgraded to the new version software, you can reconfigure the traffic groups to become active on the devices that you want by forcing the active traffic group on a device to standby state. When forcing the traffic group to standby state, you can target the device upon which you want that traffic group to run in active state. For example, you can force `traffic-group-1` on Device B into standby state, and into active state on Device A. Additionally, if you use HA groups, you can create a unique HA group for each traffic group on each device.

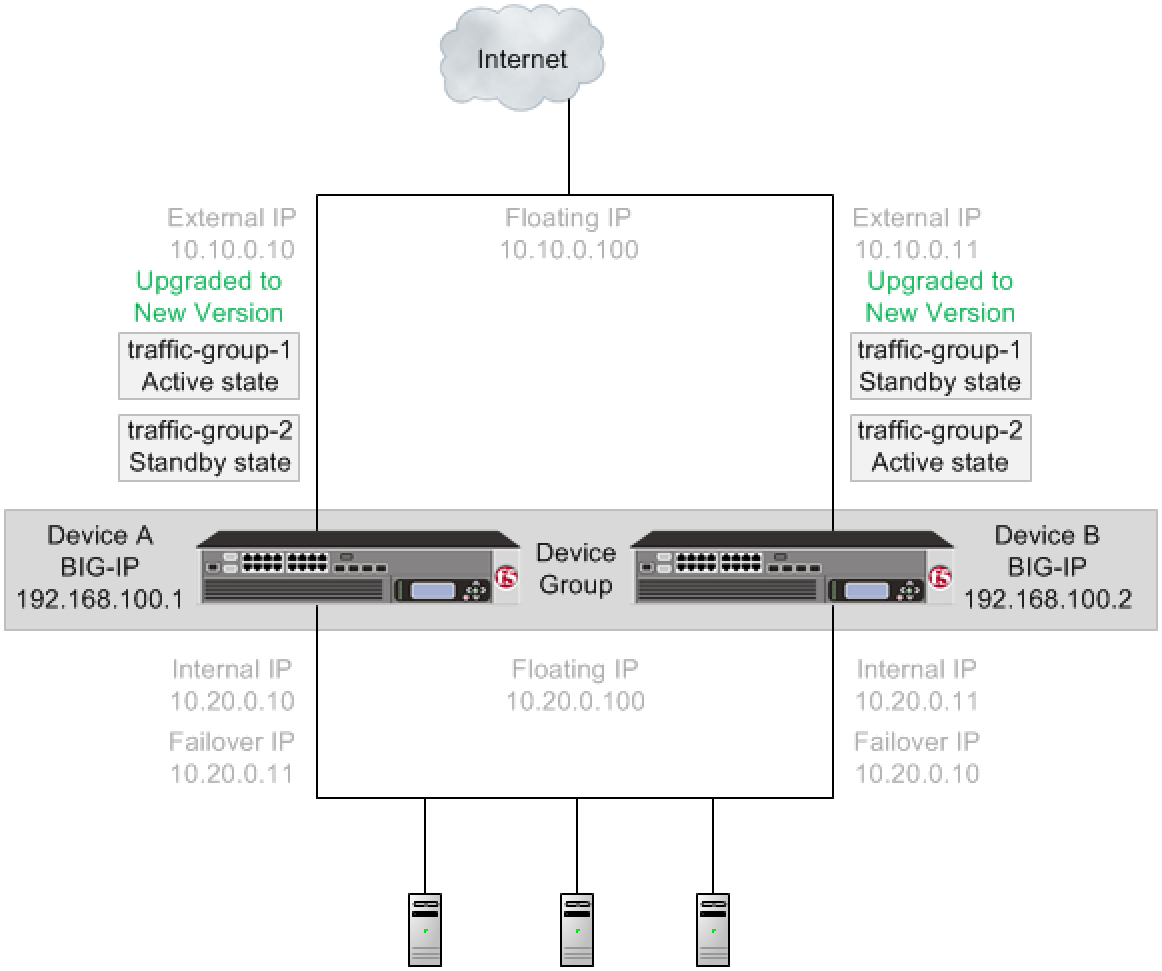

Figure 15: The new version software traffic groups in active state on two different devices

An upgrade of BIG-IP active-active systems to the new version software involves the following tasks.

Task	Description
Preparing Device A (active mode on the BIG-IP 1 system) and Device B (active mode on the BIG-IP 2 system)	In preparing to upgrade the active-active BIG-IP systems to the new version software, you need to understand any specific configuration or functional changes from the previous version, and prepare the systems. You also download the new version of software from the AskF5 web site (`www.askf5.com`) and import the files onto each device.
Forcing Device B to offline mode	When you complete preparing the Device B, you can force Device B to offline mode.
Upgrading Device B (the offline mode BIG-IP 2 system)	Once Device B is in offline mode, you can upgrade the software on that device, and reboot Device B to the location of the new version software image. Device B completes rebooting with `traffic-group1` and `traffic-group-2` in standby state. ***Important:*** *Once Device B reboots, if the BIG-IP system is configured to use a network hardware*

Task	Description
	security module (HSM), you must reinstall network HSM client software on Device B before upgrading Device A, to ensure that traffic groups using the network HSM function properly.
Forcing Device A to offline mode	When Device B completes rebooting to the location of the new version software image, you can force Device A to offline mode, changing `traffic-group-1` and `traffic-group-2` on Device B to active state.
Upgrading Device A (the offline mode BIG-IP 1 system)	Once Device A is in offline mode, you can upgrade the software on Device A. When Device A completes rebooting, traffic-group-1 and traffic-group-2 are in standby state on Device A. ***Important:** Once Device A reboots, if the BIG-IP system is configured to use a network HSM, you must reinstall network HSM client software on Device A to ensure that traffic groups using the network HSM function properly.*
Changing states of traffic groups	When you finish upgrading all of the devices, you can restore the configuration of active traffic groups on each device.
Verifying the upgrade	Finally, you should verify that your active traffic groups on the BIG-IP systems are functioning properly.
Configuring HA groups	When you finish upgrading a device, the HA group on the device (in version 11.5, and later) applies to a traffic group, as opposed to the device. You can create a unique HA group for each traffic group on each device, as necessary.
Configuring module-specific settings	According to your understanding of the configuration and functional changes from the previous version, you can reconfigure any customized module settings.

DSC components

Device service clustering (DSC®) is based on a few key components.

Devices

A *device* is a physical or virtual BIG-IP® system, as well as a member of a local trust domain and a device group. Each device member has a set of unique identification properties that the BIG-IP system generates. For device groups configured for failover, it is important that the device with the smallest capacity has the capacity to process all traffic groups. This ensures application availability in the event that all but one device in the device group become unavailable for any reason.

Device groups

A *device group* is a collection of BIG-IP devices that trust each other and can synchronize, and sometimes fail over, their BIG-IP configuration data. A *Sync-Failover* device group contains devices that synchronize configuration data and support traffic groups for failover purposes when a device becomes unavailable. The BIG-IP system supports either homogeneous or heterogeneous hardware platforms within a device group.

Important: *BIG-IP module provisioning must be equivalent on all devices within a device group. For example, module provisioning is equivalent when all device group members are provisioned to run BIG-IP® Local Traffic Manager™ (LTM®) and BIG-IP® Application Security Manager™ (ASM™) only. Maintaining equivalent module provisioning on all devices ensures that any device in the device group can process module-specific application traffic in the event of failover from another device.*

Traffic groups

A *traffic group* is a collection of related configuration objects (such as a virtual IP address and a self IP address) that run on a BIG-IP device and process a particular type of application traffic. When a BIG-IP device becomes unavailable, a traffic group can float to another device in a device group to ensure that application traffic continues to be processed with little to no interruption in service.

Device trust and trust domains

Underlying the success of device groups and traffic groups is a feature known as device trust. *Device trust* establishes trust relationships between BIG-IP devices on the network, through mutual certificate-based authentication. A *trust domain* is a collection of BIG-IP devices that trust one another and is a prerequisite for creating a device group for config sync and failover operations. The trust domain is represented by a special system-generated and system-managed device group named `device_trust_group`, which is used to synchronize trust domain information across all devices.

Folders

Folders are containers for the configuration objects on a BIG-IP device. For every administrative partition on the BIG-IP system, there is a high-level folder. At the highest level of the folder hierarchy is a folder named `root`. The BIG-IP system uses folders to affect the level of granularity to which it synchronizes configuration data to other devices in the device group.

About traffic groups

Traffic groups are the core component of failover. A *traffic group* is a collection of related configuration objects, such as a floating self IP address, a floating virtual IP address, and a SNAT translation address, that run on a BIG-IP® device. Together, these objects process a particular type of application traffic on that device.

When a BIG-IP® device goes offline, a traffic group floats (that is, fails over) to another device in the device group to make sure that application traffic continues to be processed with minimal interruption in service.

A traffic group is first active on the device you created it on. If you want an active traffic group to be active on a different device than the one you created it on, you can force the traffic group to switch to a standby state. This causes the traffic group to fail over to (and become active on) another device in the device group. The device it fails over to depends on how you configured the traffic group when you created it.

Note: *A Sync-Failover device group can support a maximum of 127 floating traffic groups.*

Task summary

The upgrade process involves preparation of the two BIG-IP® devices (Device A and Device B) configured in an active-active implementation, followed by the installation and verification of the new version software on each device. When you upgrade each device, you perform several tasks. Completing these tasks results in a successful upgrade to the new version software on both BIG-IP devices, with an active traffic group configured properly on each device.

Important: *In order to upgrade version 10.0.0 or 10.0.1 to the new version software, you must first upgrade to version 10.1.0 or 10.2.x, and then upgrade version 10.1.0 or 10.2.x to the new version software. Additionally, you can only upgrade version 10.1.0 or 10.2.x to version 12.x if you have not provisioned Global Traffic Manager™ (GTM™).*

Preparing BIG-IP modules for an upgrade from version 10.x to the new version software
Preparing RAID drives for an upgrade
Preparing BIG-IP active-active systems for an upgrade
Upgrading the active BIG-IP 2 system
Upgrading the active BIG-IP 1 system
Changing states of the traffic groups
Verifying a BIG-IP system active-active upgrade

Preparing BIG-IP modules for an upgrade from version 10.x to the new version software

Before you upgrade the BIG-IP® system from version 10.x to the new version software, you might need to manually prepare settings or configurations for specific modules.

Access Policy Manager system preparation

Access Policy Manager® is not supported in an Active-Active configuration.

Supported high availability configuration for Access Policy Manager

Access Policy Manager is supported in an Active-Standby configuration with two BIG-IP® systems only.

Important: *Access Policy Manager is not supported in an Active-Active configuration.*

Application Security Manager system preparation

The BIG-IP® Application Security Manager™ (ASM™) system does not require specific preparation when upgrading from version 10.x to the new version software. No additional configuration is required after completing the upgrade to the new software version.

What to expect after upgrading a redundant system

If you update two redundant systems that are running as an active-standby pair with BIG-IP Application Security Manager (ASM) and BIG-IP® Local Traffic Manager™ (LTM®) provisioned, the system maintains the active-standby status and automatically creates a Sync-Failover device group and a traffic group containing both systems. The device group is enabled for BIG-IP ASM (because both systems have ASM provisioned).

You can manually push or pull the updates (including BIG-IP LTM and ASM configurations and policies) from one system to the other (**Device Management** > **Overview**, click the name of a device, and choose **Sync Device to Group** or **Sync Group to Device**).

Global Traffic Manager system preparation and configuration

BIG-IP® Global Traffic Manager™ systems require specific preparation tasks and changes to upgrade from version 10.x to the new version software.

Preparation Activities

Before you upgrade Global Traffic Manager systems that are in a synchronization group, from any software version to the new version software, you must install the software on an inactive volume on each device using Live Install. After you upgrade each device, you then switch all devices to the new volume at the same time. This is required because devices in a synchronization group that includes the new version software device, cannot effectively probe each other.

Post-upgrade changes

***Important:** In BIG-IP version 12.0, BIG-IP Global Traffic Manager is renamed to BIG-IP DNS. After you upgrade, you will see the new name in the product and documentation.*

The following feature or functionality changes occur after you complete the upgrade process to the new version software:

Feature or Functionality	Description
Assigning a BIG-IP system to probe a server to gather health and performance data	Assigning a single BIG-IP system to probe a server to gather health and performance data, in version 10.x, is replaced by a Prober pool in the new software version.

Link Controller system preparation

The BIG-IP® Link Controller™ (LC™) system does not require specific preparation when upgrading from version 10.x to the new version software. No additional configuration is required after completing the upgrade to the new version software.

Local Traffic Manager system preparation

The BIG-IP® Local Traffic Manager™ (LTM®) system does not require specific preparation when upgrading from version 10.x to the new version software. No additional configuration is required after completing the upgrade to the new version software.

MAC masquerade addresses for VLANs

***Note:** If you configured **MAC Masquerade** addresses for VLANs on the version 10.x devices, one of the addresses will be included automatically in the **MAC Masquerade Address** field for **traffic-group-1** during the upgrade.*

HTTP Class profiles

F5 Networks® replaced the HTTP Class profile in BIG-IP® version 11.4.0, and later, with the introduction of the Local Traffic Policies feature. During an upgrade to BIG-IP version 11.4.0, if your configuration contains an HTTP Class profile, the BIG-IP system attempts to migrate the HTTP Class profile to an equivalent local traffic policy. For additional support information regarding the change of HTTP Class profiles to Local Traffic Policies, refer to SOL14409 on www.askf5.com.

WebAccelerator module preparation and configuration

BIG-IP® WebAccelerator modules require specific preparation tasks and changes to upgrade from version 10.x to the new version software.

Preparation activities

Before you upgrade the BIG-IP® WebAccelerator™ modules from version 10.x to an Application Acceleration Manager new software version, you need to prepare the systems, based on your configuration. The following table summarizes the applicable tasks that you need to complete.

Feature or Functionality	Preparation Task
Symmetric deployment	You must reconfigure symmetric WebAccelerator modules as asymmetric systems before you upgrade them from version 10.x to the new version software.
Unpublished policies	You must publish any policies that you want to migrate to the new software version. Only published policies are migrated into the new version software.
Signed policies	Signed policies are not supported in the new version software. If you use signed policies, you must replace them with predefined or user-defined policies before upgrading.
Configuration files	Upgrading from version 10.x to the new version software does not include custom changes to configuration files. After upgrading to the new version software, you need to manually restore any customizations made to your configuration files by using the Configuration utility or Traffic Management Shell (`tmsh`). The following list includes examples of configuration files that might have been customized: • `/config/wa/globalfragment.xml.10.x.0`; in the new software version, all `objtype` entries are provided in `tmsh`. • `/config/wa/pvsystem.conf.10.x.0` • `/config/wa/pvsystem.dtd.10.x.0` • `/config/wa/transforms/common.zip.10.x.0`; the new software version does not include transforms.
Debug Options	`X-PV-Info` response headers in version 10.x are changed to `X-WA-Info` response headers in the new software version. The default setting for **X-WA-Info Headers** is **None** (disabled). To use `X-WA-Info` response headers, you will need to change this setting, and update any associated iRules® or scripts, accordingly.

Post-upgrade activities

When you complete upgrading to the new version software, you should consider the following feature or functionality changes that occur for the Application Acceleration Manager modules. Depending upon your configuration, you might need to perform these changes after you upgrade the systems.

Feature or Functionality	Description
Web acceleration	Web acceleration functionality requires configuration of the Web Acceleration profile. ***Important:*** *You must enable an Application Acceleration Manager module application in the Web Acceleration profile to enable the Application Acceleration Manager module.*
Compression	Compression functionality requires configuration of the HTTP Compression profile in the new version software.
Request logging	Request logging does not migrate to the new version software. You must recreate the configuration after upgrading by using the Request Logging profile.
Policy logging	Policy logging does not migrate to the new version software. You must recreate the configuration after upgrading by using the Request Logging profile.
URL normalization	URL normalization is not supported in the new version software.
ESI functionality	Edge Side Include (ESI) functionality in the Application Acceleration Manager module is not supported in the new version software, with the exception of ESI invalidations.
iControl® backward compatibility	Backward compatibility for iControl Compression and RAM Cache API settings in the HTTP profile is not supported in the new version software. These settings appear in the HTTP Compression and Web Acceleration profiles in the new software version.

WAN Optimization Manager preparation

BIG-IP® WAN Optimization Manager™ (WOM®) systems do not require specific preparation when upgrading from version 10.x to the new version software. However, in a redundant system configuration, you must upgrade the standby system first (to avoid interrupting traffic on the active system), and then upgrade the other system. No additional configuration is required after completing the upgrade to the new version software.

Preparing RAID drives for an upgrade

If your configuration includes redundant array of independent disks (RAID) drives, you need to verify that the RAID drives are ready for upgrading. If a RAID drive shows errors before upgrading, you will want to contact F5 customer support to resolve the errors before initiating the upgrade.

1. Open the Traffic Management Shell (tmsh).
   `tmsh`
   This starts `tmsh` in interactive shell mode and displays the `tmsh` prompt: `(tmos)#`.
2. Verify the health of RAID disks, ensuring that the drives are not failed or undefined.

   ```
   (tmos)# show sys raid
   ```

```
Sys::Raid::Array: MD1
--------------------
Size (MB) 305245

Sys::Raid::ArrayMembers
Bay ID Serial Number Name Array Member Array Status
---------------------------------------------------------
1 WD-WCAT18586780 HD2 yes failed
2 WD-WCAT1E733419 HD1 yes ok
```

In this example, the array is labeled MD1 and disk HD2 indicates an error.

3. Verify `Current_Pending_Sector` data displays a `RAW_VALUE` entry of less than `1` on RAID systems.

Option	Description
For version 11.4.0, and later	Run the platform check utility: `(tmos)# run util platform_check`
For version 11.3.x, and earlier	At the command line, run the smartctl utility: `smartctl -t long -d ata /dev/<sda|sdb|hda|hdc>`

```
197 Current_Pending_Sector  0x0032  200  200  000  Old_age  Always  -  0
```

In this example, the `RAW_VALUE` entry is `0`.

4. Verify that no known issues appear in the following log files.
   - Check `/var/log/user.log` for LBA messages indicating failure to recover, for example, `recovery of LBA:226300793 not complete`.
   - Check `/var/log/kern.log` for ATA error entries.

The health of all RAID drives is assessed, enabling you to resolve any issues before proceeding with the BIG-IP® software upgrade.

Preparing BIG-IP active-active systems for an upgrade

The following prerequisites apply when you upgrade BIG-IP® active-active devices from version 10.x to the new version software.

- The BIG-IP systems (Device A and Device B) are configured as an active-active pair.
- Each BIG-IP device is running the same version of 10.x software.
- The BIG-IP active-active devices are the same model of hardware.

When you upgrade a BIG-IP active-active pair from version 10.x to the new version software, you begin by preparing the devices.

***Note:** If you prefer to closely observe the upgrade of each device, you can optionally connect to the serial console port of the device that you are upgrading.*

1. For each device, complete the following steps to prepare the configuration and settings.
   a) Examine the Release Notes for specific configuration requirements, and reconfigure the systems, as necessary.

      For example, you must reconfigure version 10.x symmetric WebAccelerator modules as asymmetric systems before upgrading to the new version software.

   b) Examine the Release Notes for specific changes to settings that occur when upgrading from version 10.x to the new version software, and complete any in-process settings.

      For example, you must publish any unpublished BIG-IP® WebAccelerator™ module policies in order for them to migrate to the new version software.

2. From the device that is running the latest configuration, synchronize the configuration to the peer unit.
   a) On the Main menu, click **System** > **High Availability** > **ConfigSync**.
   A message appears for the Status Message.
   b) Click **Synchronize TO Peer**.
3. For each device, click **System** > **High Availability** > **Redundancy**, and, from the **Redundancy State Preference** list, select **None**.
4. For each device, create a backup file.
   a) Access the `tmsh` command line utility.
   b) At the prompt, type `save /sys ucs /shared/filename.ucs`.
   c) Copy the backup file to a safe location on your network.
5. Download the BIG-IP new version software `.iso` file, and, if available, latest hotfix `.iso` file from the AskF5™ downloads web site (`https://downloads.f5.com`) to a preferred location.
6. Import either the latest BIG-IP system hotfix image file, if available, or the new version software upgrade image file to each device.

Option	Description
Import the latest BIG-IP system hotfix image and SIG file	1. On the Main menu, click **System** > **Software Management** > **Hotfix List** > **Import**. 2. Click **Browse**, locate and click the SIG file (Hotfix-BIGIP-hf-xx.x.x.x.x.xxxx.HFx.iso.384.sig), click **Open**, and click **Import**. 3. Click **Browse**, locate and click the image file, click **Open**, and click **Import**. 4. When the hotfix image file completes uploading to the BIG-IP device, click **OK**. A link to the image file appears in the Software Image list.
Import the new version software image and SIG file	1. On the Main menu, click **System** > **Software Management** > **Image List** > **Import**. 2. Click **Browse**, locate and click the SIG file (BIGIP-13.x.x.x.x.xxxx.iso.384.sig), click **Open**, and click **Import**. 3. Click **Browse**, locate and click the upgrade image file, click **Open**, and click **Import**. ***Note:*** *BIG-IP version 13.x, and later, provides upgrade and recovery image files. An upgrade image file (for example, BIGIP-13.x.x.x.x.xxx.iso) omits End User Diagnostics (EUD) software, which includes tests that report on hardware components. A recovery image file (for example, BIGIP-RECOVERY-13.x.x.x.x.xxx.iso) includes EUD software.* 4. When the software image file completes uploading to the BIG-IP device, click **OK**. A link to the image file appears in the Software Image list.

7. (Optional) Verify the integrity of the imported software image file.

Option	Description
Use SIG verification (recommended)	1. At the command line, determine the filename of the applicable public key file. Example: `# ls /usr/lib/install/archive.pubkey*pem`. The list of `archive.pubkey` files appears. 2. Using the openssl utility, verify the integrity of the imported software image file.

Option	Description
	Example: `# openssl dgst -sha384 -verify usr/lib/install/archive.pubkey.xxxxxxxxx.pem -signature shared/images/BIGIP-13.x.x.x.x.xxxx.iso.384.sig shared/images/BIGIP-13.x.x.x.x.xxxx.iso` ***Note:*** *You must use openssl version 1.0.0, or later. Type* `openssl version` *at the command line to determine the version.* The openssl utility verifies the integrity of the software image file and displays the results. # openssl dgst -sha384 -verify usr/lib/install/archive.pubkey.xxxxxxxxx.pem -signature shared/images/BIGIP-13.x.x.x.x.xxxx.iso.384.sig shared/images/BIGIP-13.x.x.x.x.xxxx.iso Verified OK
Use an MD5 checksum	• Using a tool or utility that computes an md5 checksum, you can verify the integrity of the BIG-IP system latest hotfix `.iso` file or new version `.iso` file.

The BIG-IP devices are now prepared to install the latest hotfix or new version software onto Device B (the active BIG-IP 2 device).

Upgrading the active BIG-IP 2 system

The following prerequisites apply for this task.

- Device A (the active BIG-IP® 1 system) and Device B (the active BIG-IP 2 system) must be prepared to upgrade Device B with the new version software.
- Either the latest hotfix image file, if available, or the new version software image file is downloaded and accessible.

After you prepare Device A (the active BIG-IP 1 system) and Device B (the active BIG-IP 2 system) for upgrading the software, you can perform these steps to install the new version software onto Device B.

1. Force Device B to offline mode.
   a) On the Main menu, click **System** > **High Availability** > **Redundancy**.
   b) Click **Force Offline**.
      The BIG-IP device (Device B) changes to offline mode.
2. Reactivate the software license.
   a) On the Main menu, click **System** > **License**.
   b) Click **Re-activate**.
   c) In the **Activation Method** area, select the **Automatic (requires outbound connectivity)** option.
   d) Click **Next**.

      The BIG-IP software license renews automatically.
   e) Click **Continue**.
3. Install either the latest hotfix image, if available, or the new version software.

Option	Description
Install the latest hotfix image	**1.** On the Main menu, click **System** > **Software Management** > **Hotfix List**.

Option	Description
	2. In the Available Images area, select the check box for the hotfix image, and click **Install**. The Install Software Hotfix popup screen opens. **3.** From the **Volume set name** list, select the location of the new version software volume to install the hotfix image, and click **Install**. ***Important:*** *In the* ***Install Status*** *list for the specified location, a progress bar indicates the status of the installation. Ensure that installation successfully completes, as indicated by the progress bar, before proceeding.*
Install the new version software	**1.** On the Main menu, click **System** > **Software Management** > **Image List**. **2.** In the Available Images area, select the check box for the new version software image, and click **Install**. The Install Software Image popup screen opens. **3.** From the **Volume set name** list, select a location to install the image, and click **Install**. ***Important:*** *In the* ***Install Status*** *list for the specified location, a progress bar indicates the status of the installation. Ensure that installation successfully completes, as indicated by the progress bar, before proceeding.*

4. Reboot the device to the location of the installed new version software image.

a) On the Main menu, click **System** > **Software Management** > **Boot Locations**.
b) In the **Boot Location** list, click the boot location of the installed new version software image.
c) Click **Activate**.

The BIG-IP device reboots to the new version software boot location.

Note: *If the device appears to be taking a long time to reboot, do not cycle the power off and on. Instead, verify the status of the device by connecting to its serial console port. The device might be performing firmware upgrades.*

The new version software is installed on Device B, with `traffic-group-1` and `traffic-group-2` in standby state.

Upgrading the active BIG-IP 1 system

The following prerequisites apply in upgrading Device A (the BIG-IP® 1 system).

- Device A (the version 10.x BIG-IP 1 system) must be prepared to upgrade the software to the new version software.
- Device A is in active mode.
- Device B (the new version software BIG-IP device with `traffic-group-1` and `traffic-group-2` in standby state) is in standby state.
- Either the latest hotfix image file, if available, or the new version software image file is downloaded and accessible.

After you prepare Device A (the active BIG-IP 1 system) for upgrading the software, you can perform these steps to upgrade the software to the new version software.

1. Force Device A to offline mode.

a) On the Main menu, click **System** > **High Availability** > **Redundancy**.
b) Click **Force Offline**.
The BIG-IP device (Device B) changes to offline mode.

2. Reactivate the software license.
   a) On the Main menu, click **System** > **License**.
   b) Click **Re-activate**.
   c) In the **Activation Method** area, select the **Automatic (requires outbound connectivity)** option.
   d) Click **Next**.

      The BIG-IP software license renews automatically.
   e) Click **Continue**.
3. Install either the latest hotfix image, if available, or the new version software.

Option	Description
Install the latest hotfix image	**1.** On the Main menu, click **System** > **Software Management** > **Hotfix List**. **2.** In the Available Images area, select the check box for the hotfix image, and click **Install**. The Install Software Hotfix popup screen opens. **3.** From the **Volume set name** list, select the location of the new version software volume to install the hotfix image, and click **Install**. ***Important:*** *In the* ***Install Status*** *list for the specified location, a progress bar indicates the status of the installation. Ensure that installation successfully completes, as indicated by the progress bar, before proceeding.*
Install the new version software	**1.** On the Main menu, click **System** > **Software Management** > **Image List**. **2.** In the Available Images area, select the check box for the new version software image, and click **Install**. The Install Software Image popup screen opens. **3.** From the **Volume set name** list, select a location to install the image, and click **Install**. ***Important:*** *In the* ***Install Status*** *list for the specified location, a progress bar indicates the status of the installation. Ensure that installation successfully completes, as indicated by the progress bar, before proceeding.*

4. Reboot the BIG-IP device (Device A) to the location of the installed new version software image.

   Important: *Once Device A reboots, if the BIG-IP system is configured to use a network HSM, you must reinstall network HSM client software on Device A to ensure that traffic groups using the network HSM function properly.*

   a) On the Main menu, click **System** > **Software Management** > **Boot Locations**.
   b) In the Boot Location list, click the boot location of the installed new version software image.
   c) Click **Activate**.

      The BIG-IP device (Device A) reboots to the new version software boot location with `traffic-group-1` and `traffic-group-2` in standby state.

      Note: *If the device appears to be taking a long time to reboot, do not cycle the power off and on. Instead, verify the status of the device by connecting to its serial console port. The device might be performing firmware upgrades.*
5. On the Main tab, click **Device Management** > **Overview**.
6. In the Devices area of the screen, choose the device that shows a sync status of `Changes Pending`.
7. In the Sync Options area of the screen, select **Push the selected device configuration to the group**.
8. Click **Sync**.

The new version software is now installed on Device A, with `traffic-group-1` and `traffic-group-2` in standby state.

Changing states of the traffic groups

Manually configuring active state traffic groups across devices within a device group involves forcing an active state traffic group on a device to standby state, and retargeting that active state traffic group to a different device. Completing these tasks results in active state traffic groups on the appropriate devices in a device group.

Viewing a list of traffic groups for a device

You can view a list of traffic groups for the device group. Using this list, you can add floating IP addresses to a traffic group, force a traffic group into a Standby state, and view information such as the current and next-active devices for a traffic group and its HA load factor.

1. On the Main tab, click **Device Management** > **Traffic Groups**.
2. In the Name column, view the names of the traffic groups on the local device.

Forcing a traffic group to a standby state

You perform this task when you want the selected traffic group on the local device to fail over to another device (that is, switch to a `Standby` state). Users typically perform this task when no automated method is configured for a traffic group, such as auto-failback or an HA group. By forcing the traffic group into a `Standby` state, the traffic group becomes active on another device in the device group. For device groups with more than two members, you can choose the specific device to which the traffic group fails over.

1. Log in to the device on which the traffic group is currently active.
2. On the Main tab, click **Device Management** > **Traffic Groups**.
3. In the Name column, locate the name of the traffic group that you want to run on the peer device.
4. Select the check box to the left of the traffic group name.

   If the check box is unavailable, the traffic group is not active on the device to which you are currently logged in. Perform this task on the device on which the traffic group is active.
5. Click **Force to Standby**.
   This displays target device options.
6. Choose one of these actions:

   - If the device group has two members only, click **Force to Standby**. This displays the list of traffic groups for the device group and causes the local device to appear in the Next Active Device column.
   - If the device group has more than two members, then from the **Target Device** list, select a value and click **Force to Standby**.

The selected traffic group is now in a standby state on the local device and active on another device in the device group.

Verifying a BIG-IP system active-active upgrade

Prerequisite: You must complete a software upgrade of the BIG-IP® active-active pair from version 10.x to the new version software.

When you have completed upgrading the BIG-IP active-active pair from version 10.x to the new version software, you should verify that the upgraded configuration is working properly. Perform the following steps to verify the new version software upgrade.

1. Verify the Platform configuration for each device.
   a) On the Main menu, click **System** > **Platform**.
   b) For the **Root Folder Device Group** setting, verify that the device group is identical on the pair of devices.
   c) From the **Root Folder Group** list, verify that the correct traffic group (**traffic-group-1**) is selected.
2. Verify the configuration for each device.
   a) On the Main menu, click **Device Management** > **Devices**.
   b) Verify the following information for the device and the peer device.
      - active-active status
      - device name
      - management IP address
      - hostname
      - TMOS version
   c) On the Main menu, click **Device Management** > **Device Trust** > **Peer List**.
   d) Verify that the peer device is specified as a Peer Authority Device.

   Note: *Ensure that all information for the peer device appears correctly and complete.*
3. Verify the traffic groups for each device.
   a) On the Main menu, click **Device Management** > **Traffic Groups**.
   b) Click **traffic-group-1**.
   c) If you configured **MAC Masquerade** addresses for VLANs on the version 10.x devices, verify that the **traffic-group-1** includes an address in the **MAC Masquerade Address** field.
   d) Click **traffic-group-2**.
   e) If you configured **MAC Masquerade** addresses for VLANs on the version 10.x devices, verify that the **traffic-group-2** includes an address in the **MAC Masquerade Address** field.
   f) Verify that the floating traffic group is correct.
   g) Verify that the failover objects are correct.
4. Verify the Current ConfigSync State for each device.
   a) On the Main menu, click **Device Management** > **Overview**.
   b) In the Devices area of the screen, in the Sync Status column, verify that each device shows a sync status of green.

The upgraded system is verified and working properly.

Implementation result

Your upgrade of the BIG-IP® active-active pair from version 10.x to the new version software is now complete. The new version software configuration includes a device group with two devices (Device A and Device B) and two traffic groups (`traffic-group-1` and `traffic-group-2`), with the first traffic group (`traffic-group-1`) on one device (Device A) in active state and the second traffic group (`traffic-group-2`) on the other device (Device B) in active state.

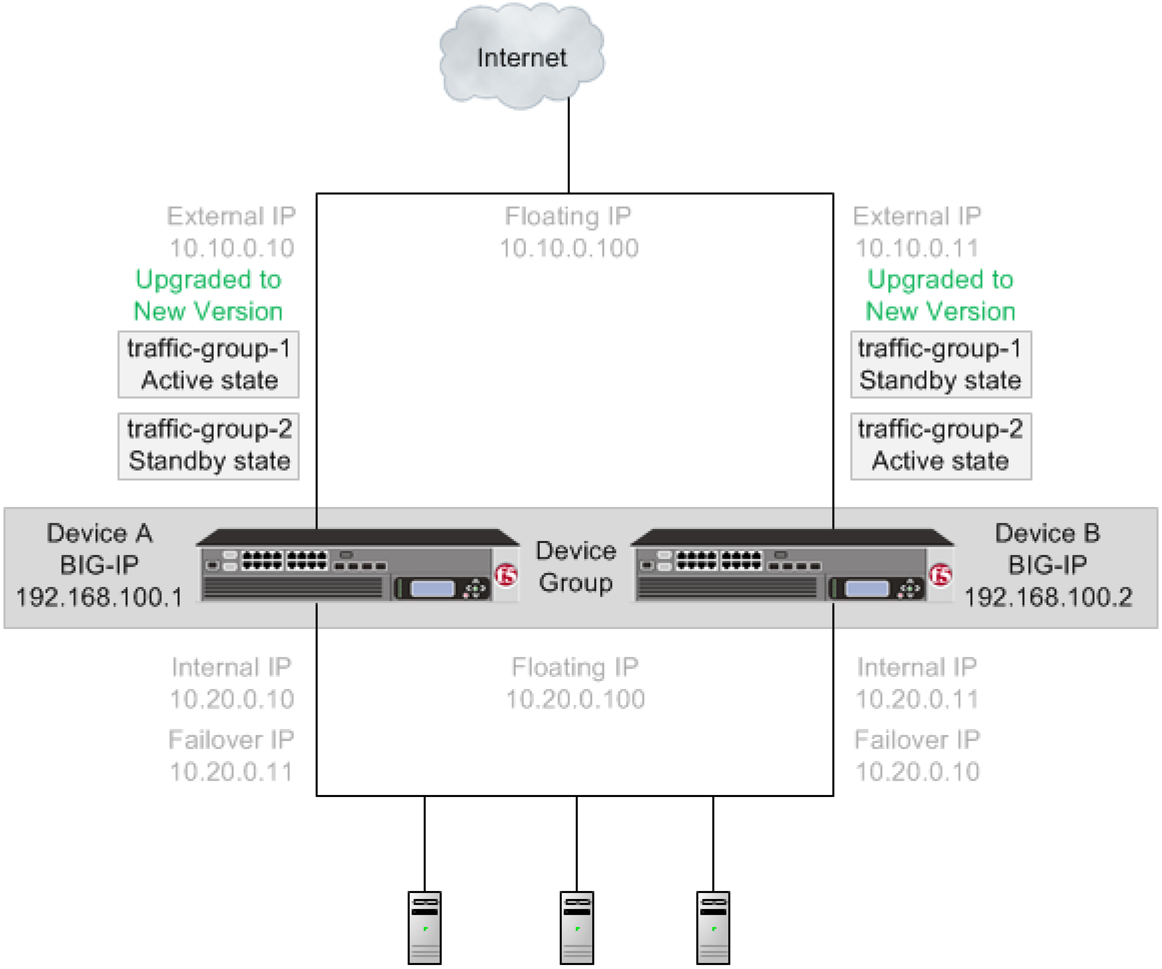

Figure 16: The new version software device group and two traffic groups in active state on different devices

Legal Notices

Legal notices

Publication Date

This document was published on March 2, 2017.

Publication Number

MAN-0587-01

Copyright

F5 Networks, Inc. (F5) believes the information it furnishes to be accurate and reliable. However, F5 assumes no responsibility for the use of this information, nor any infringement of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent, copyright, or other intellectual property right of F5 except as specifically described by applicable user licenses. F5 reserves the right to change specifications at any time without notice.

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*.

Link Controller Availability

This product is not currently available in the U.S.

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