BIG-IP® System: Upgrading Active-Standby Systems

11.0

Table of Contents

Legal Notices

Publication Date

This document was published on September 24, 2015.

Publication Number

MAN-0374-00

Copyright

Copyright © 2012-2015, F5 Networks, Inc. All rights reserved.

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

3DNS, Access Policy Manager, Acopia, Acopia Networks, Advanced Client Authentication, Advanced Routing, APM, Application Security Manager, ARX, AskF5, ASM, BIG-IP, Cloud Extender, CloudFucious, CMP, Data Manager, DevCentral, DevCentral [DESIGN], DNS Express, DSC, DSI, Edge Client, Edge Gateway, Edge Portal, EM, Enterprise Manager, F5, F5 [DESIGN], F5 Management Pack, F5 Networks, F5 World, Fast Application Proxy, Fast Cache, FirePass, Global Traffic Manager, GTM, IBR, Intelligent Browser Referencing, Intelligent Compression, IPv6 Gateway, iApps, iControl, iHealth, iQuery, iRules, iRules OnDemand, iSession, IT agility. Your way., L7 Rate Shaping, LC, Link Controller, Local Traffic Manager, LTM, Message Security Module, MSM, Netcelera, OneConnect, Packet Velocity, Protocol Security Module, PSM, Real Traffic Policy Builder, Scale^{N}, SSL Acceleration, StrongBox, SuperVIP, SYN Check, TCP Express, TDR, TMOS, Traffic Management Operating System, TrafficShield, Transparent Data Reduction, VIPRION, vCMP, WA, WAN Optimization Manager, WANJet, WebAccelerator, WOM, and ZoneRunner, are trademarks or service marks of F5 Networks, Inc., in the U.S. and other countries, and may not be used without F5's express written consent.

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:
http://www.f5.com/about/guidelines-policies/patents

Export Regulation Notice

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

RF Interference Warning

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

FCC Compliance

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

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

Canadian Regulatory Compliance

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

Standards Compliance

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

Acknowledgments

This product includes software developed by Bill Paul.

This product includes software developed by Jonathan Stone.

This product includes software developed by Manuel Bouyer.

This product includes software developed by Paul Richards.

This product includes software developed by the NetBSD Foundation, Inc. and its contributors.

This product includes software developed by the Politecnico di Torino, and its contributors.

This product includes software developed by the Swedish Institute of Computer Science and its contributors.

This product includes software developed by the University of California, Berkeley and its contributors.

This product includes software developed by the Computer Systems Engineering Group at the Lawrence Berkeley Laboratory.

This product includes software developed by Christopher G. Demetriou for the NetBSD Project.

This product includes software developed by Adam Glass.

This product includes software developed by Christian E. Hopps.

This product includes software developed by Dean Huxley.

This product includes software developed by John Kohl.

This product includes software developed by Paul Kranenburg.

This product includes software developed by Terrence R. Lambert.

This product includes software developed by Philip A. Nelson.

This product includes software developed by Herb Peyerl.

This product includes software developed by Jochen Pohl for the NetBSD Project.

This product includes software developed by Chris Provenzano.

This product includes software developed by Theo de Raadt.

This product includes software developed by David Muir Sharnoff.

This product includes software developed by SigmaSoft, Th. Lockert.

This product includes software developed for the NetBSD Project by Jason R. Thorpe.

This product includes software developed by Jason R. Thorpe for And Communications, http://www.and.com.

This product includes software developed for the NetBSD Project by Frank Van der Linden.

This product includes software developed for the NetBSD Project by John M. Vinopal.

This product includes software developed by Christos Zoulas.

This product includes software developed by the University of Vermont and State Agricultural College and Garrett A. Wollman.

This product includes software developed by Balazs Scheidler (bazsi@balabit.hu), which is protected under the GNU Public License.

This product includes software developed by Niels Mueller (nisse@lysator.liu.se), which is protected under the GNU Public License.

In the following statement, *This software* refers to the Mitsumi CD-ROM driver: This software was developed by Holger Veit and Brian Moore for use with 386BSD and similar operating systems. *Similar operating systems* includes mainly non-profit oriented systems for research and education, including but not restricted to NetBSD, FreeBSD, Mach (by CMU).

This product includes software developed by the Apache Group for use in the Apache HTTP server project (http://www.apache.org/).

This product includes software licensed from Richard H. Porter under the GNU Library General Public License (© 1998, Red Hat Software), www.gnu.org/copyleft/lgpl.html.

This product includes the standard version of Perl software licensed under the Perl Artistic License (© 1997, 1998 Tom Christiansen and Nathan Torkington). All rights reserved. You may find the most current standard version of Perl at http://www.perl.com.

This product includes software developed by Jared Minch.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product contains software based on oprofile, which is protected under the GNU Public License.

This product includes RRDtool software developed by Tobi Oetiker (http://www.rrdtool.com/index.html) and licensed under the GNU General Public License.

This product contains software licensed from Dr. Brian Gladman under the GNU General Public License.

This product includes software developed by the Apache Software Foundation (http://www.apache.org/).

This product includes Hypersonic SQL.

This product contains software developed by the Regents of the University of California, Sun Microsystems, Inc., Scriptics Corporation, and others.

This product includes software developed by the Internet Software Consortium.

This product includes software developed by Nominum, Inc. (http://www.nominum.com).

This product contains software developed by Broadcom Corporation, which is protected under the GNU Public License.

This product contains software developed by MaxMind LLC, and is protected under the GNU Lesser General Public License, as published by the Free Software Foundation.

This product includes software developed by the Computer Systems Engineering Group at Lawrence Berkeley Laboratory. Copyright ©1990-1994 Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: This product includes software developed by the Computer Systems Engineering Group at Lawrence Berkeley Laboratory.
4. Neither the name of the University nor of the Laboratory may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY

DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes software developed by Sony Computer Science Laboratories Inc. Copyright © 1997-2003 Sony Computer Science Laboratories Inc. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY SONY CSL AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL SONY CSL OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Chapter 1

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.*

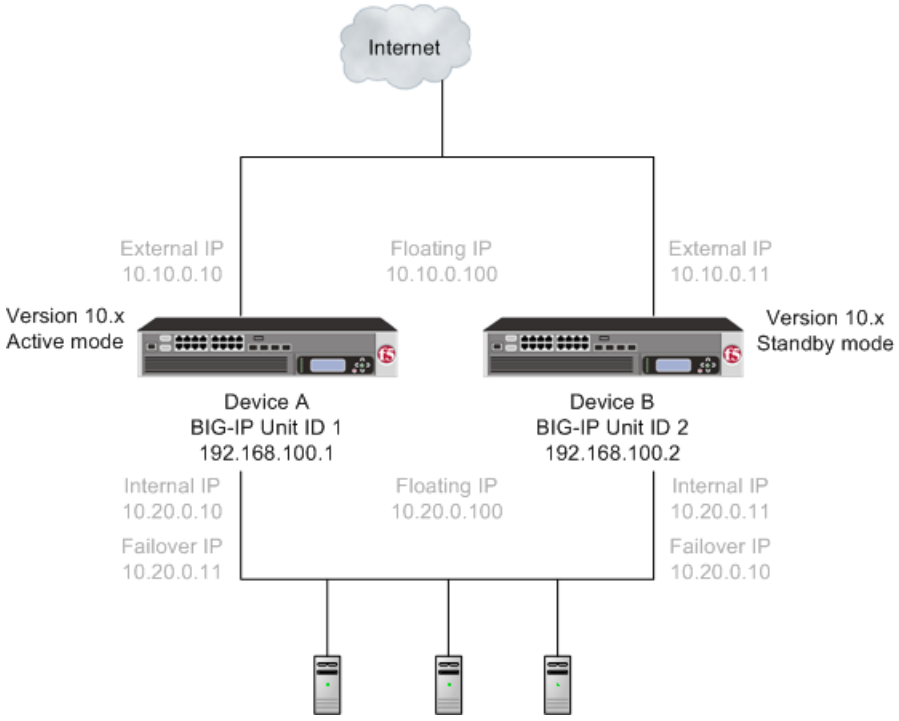

Figure 1: A version 10.x active-standby pair

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.*

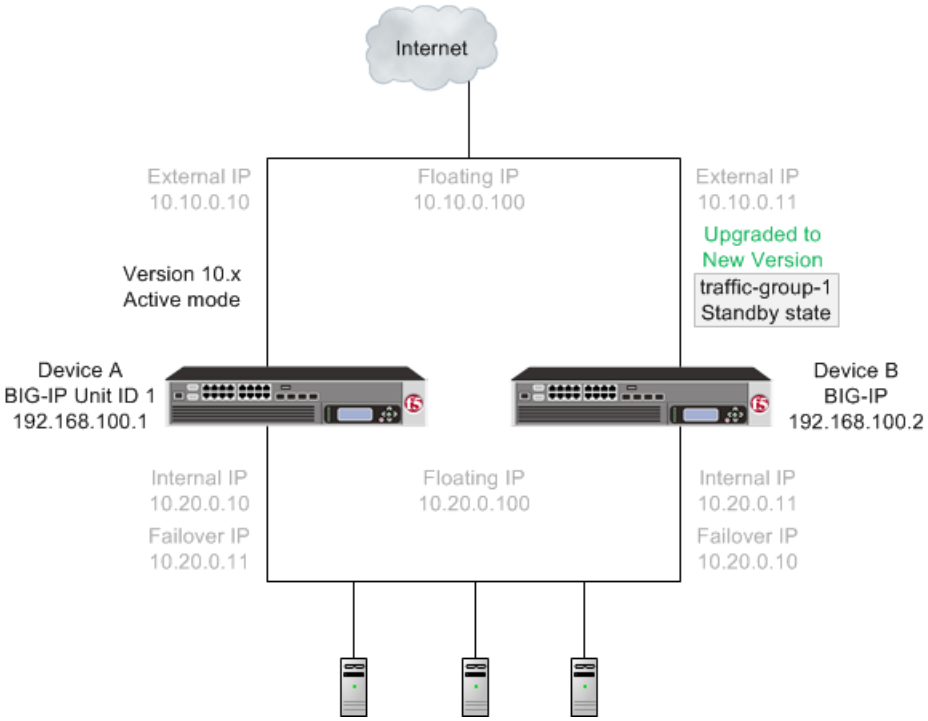

Figure 2: A version 10.x device in active mode and a new software version traffic group in standby state

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.

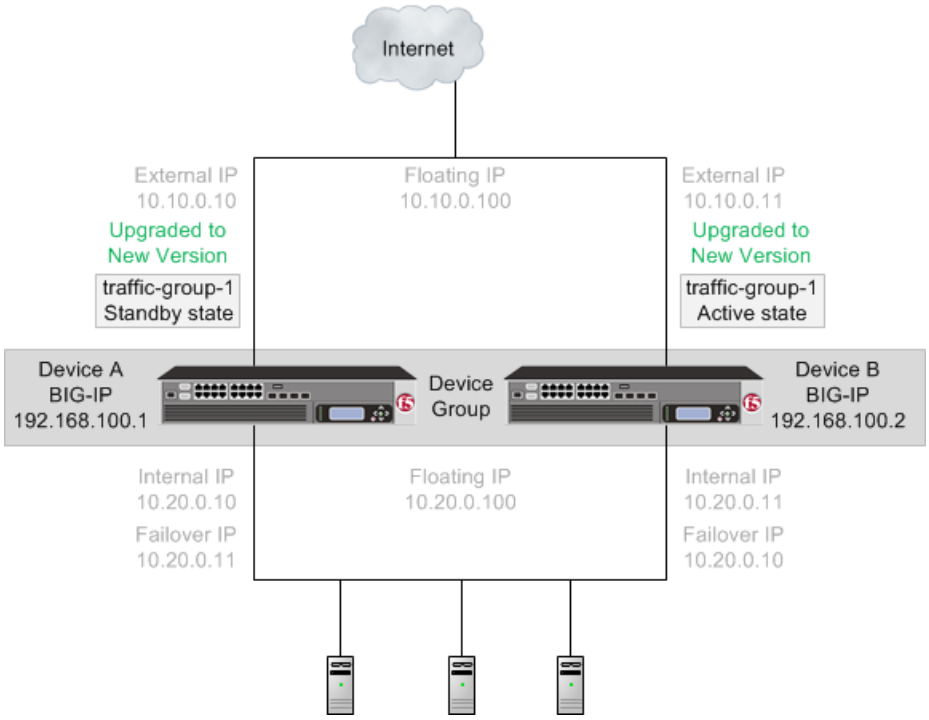

Figure 3: A new version software traffic group in active and standby states

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 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

Task	Description
	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.

Configuration components

BIG-IP® redundant system configuration 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.

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.

Important: *To configure redundancy on a device, you do not need to explicitly specify that you want the BIG-IP device to be part of a redundant configuration. Instead, this occurs automatically when you add the device to an existing device group.*

You can create two types of devices groups:

Sync-Failover

A *Sync-Failover* device group contains devices that synchronize configuration data and support traffic groups for failover purposes when a device becomes unavailable. Devices in a Sync-Failover device group must match with respect to hardware platform, product licensing, and module provisioning.

Sync-Only

A *Sync-Only* device group contains devices that synchronize configuration data, such as policy data, but do not synchronize failover objects.

A BIG-IP device can be a member of only one Sync-Failover group. However, a device can be a member of both a Sync-Failover device group and a Sync-Only device group.

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 successful operation 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 can therefore synchronize and fail over their BIG-IP configuration data, as well as exchange status and failover messages on a regular basis. A *local trust domain* is a trust domain that includes the local device, that is, the device you are currently logged in to.

Folders and sub folders

Folders and *sub-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. You can create sub-folders within a high-level folder, using `tmsh`.

Note: *In most cases, you can manage redundancy for all device group members remotely from one specific member. However, there are cases when you must log in locally to a device group member to perform a task. An example is when resetting device trust on a device.*

About traffic groups

A *traffic group* is a collection of related configuration objects that run on a BIG-IP® device. Together, these objects process a particular type of traffic on that device. When a BIG-IP device becomes unavailable, a traffic group floats (that is, fails over) to another device in a device group to ensure that application traffic continues to be processed with little to no interruption in service. In general, a traffic group ensures that when a device becomes unavailable, all of the failover objects in the traffic group fail over to any one of the devices in the device group, based on the current workload of those devices.

Important: *Although a specific traffic group can be active on only one device in a device group, the traffic group actually resides and is in a standby state on all other device group members, due to configuration synchronization.*

Only certain types of configuration objects can belong to a traffic group. Examples of traffic group objects are self IP addresses and virtual IP addresses.

An example of a set of objects in a traffic group is an iApps™ application service. If a device with this traffic group is a member of a device group, and the device becomes unavailable, the traffic group floats to another member of the device group, and that member becomes the device that processes the application traffic.

When a traffic group fails over to another device in the device group, the device that the system selects to run the traffic group is normally the device that is most available from a workload perspective. However, when you initially create the traffic group on a device, you specify the device in the group that you prefer that traffic group to run on whenever possible.

Note: *A Sync-Failover device group can support a maximum of 15 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.*

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

Feature or Functionality	Description

	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 {`
	
	`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** > **Device Groups**, then click **Config Sync** and choose **Synchronize TO/FROM Group**).

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

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.*

Protocol Security Manager preparation

The BIG-IP® Protocol Security Manager™ (PSM™) 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.

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 WebAccelerator™ modules from version 10.x to the 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. 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 a WebAccelerator application in the Web Acceleration profile to enable the WebAccelerator system.*
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 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. Using a tool or utility that computes an md5 checksum, verify the integrity of the downloaded BIG-IP `.iso` file.
7. Import either the latest BIG-IP hotfix image file, if available, or the new version software image file to each device.

Option	Description
Import the latest BIG-IP system hotfix image file	**1.** On the Main menu, click **System** > **Software Management** > **Hotfix List** > **Import**. **2.** Click **Browse**, locate and click the image file, click **Open**, and click **Import**. **3.** 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 file	**1.** On the Main menu, click **System** > **Software Management** > **Image List** > **Import**. **2.** Click **Browse**, locate and click the image file, click **Open**, and click **Import**. **3.** 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.

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. Synchronize the configuration.
   a) On the Main tab, click **Device Management** > **Device Groups**
   b) Click the name of a device group.
   c) On the menu bar, click **Config Sync**.

   The Config Sync screen appears, displaying the status for each member.
   d) As indicated by the Status Message, click one of the following buttons.
      - **Synchronize TO Group**
      - **Synchronize FROM Group**

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 **Network** > **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** > **Devices**.
   b) In the Device List, in the 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.

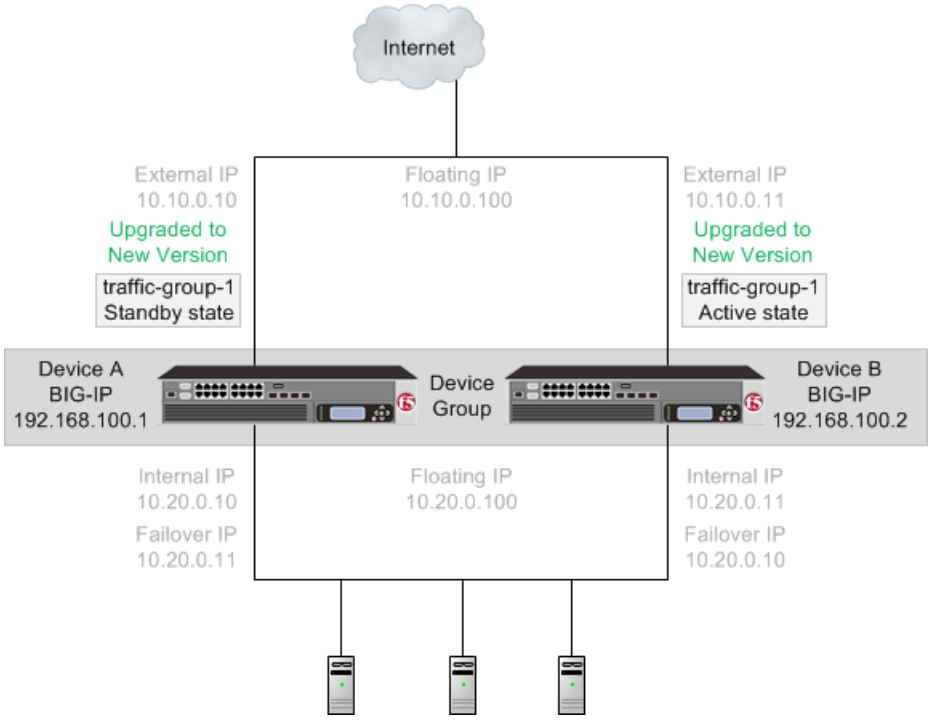

Figure 4: A new version software device group and traffic group

Index