BIG-IP® System: Migrating Devices

Version 12.1.3

Table of Contents

Migration of Devices Running Different Version Software

About migrating devices running different software versions

What is device migration?

Device migration enables you to replace the devices in a BIG-IP® device group running earlier version software with newer upgraded devices running software version 12.1.3, or later. It enables you to take an existing configuration on a device group's source device and easily replicate it on a newer target device.

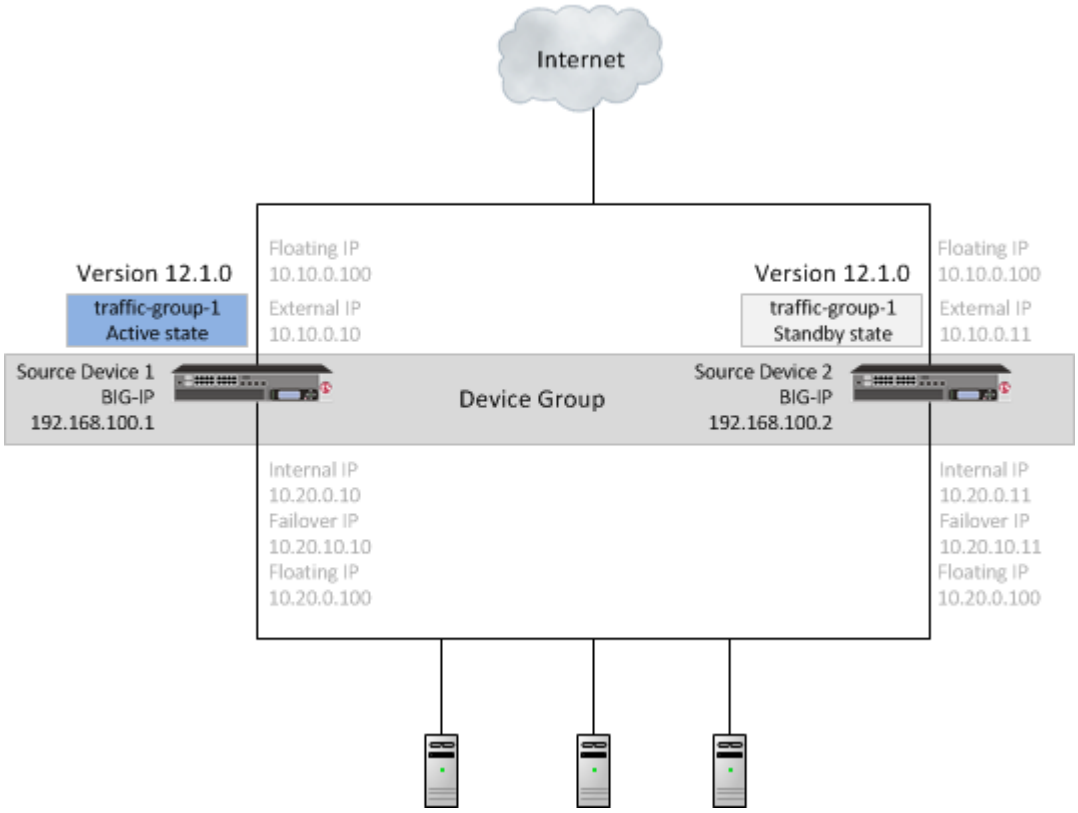

Figure 1: Source devices in a device group

Supported platforms

Supported source and target platforms include appliances, VIPRION® platforms, virtual edition (VE) devices, and vCMP® guests.

Supported software versions

You can migrate the configuration of any BIG-IP version 11.x.x, 12.0.0, 12.1.0, or 12.1.2 source device to a BIG-IP version 12.1.3, or later, target device.

Configuration Dependencies

Migration to newer devices running software version 12.1.3, or later, ignores the following configuration objects. If your configuration includes dependencies on any of these objects, you must reconfigure them on the new device before you load the UCS file onto that device.

Important: *You must reconfigure the following objects on the new target device to use the same names as the objects on the source device, before you load the UCS file onto that device*

- Interfaces
- Interface bundles
- Management IP address
- Management route

Migration of a device group to newer devices

When you migrate the source devices in a device group running earlier version software to new target devices running BIG-IP® software version 12.1.3, or later, the following sequence of steps applies. This sequence migrates a device group composed of source devices 1 and 2 to a device group composed of new target devices 1 and 2.

Important:

- For a device group, migration functionality reestablishes the device group with the target devices when you load an archive onto the second target device.
- During migration, do not make any additional configuration changes. Reconfiguration during migration can cause unexpected behavior.
- Devices run different software versions during migration, preventing normal config sync functionality until migration completes.

Step 1. Migrate source device 1 to target device 1.

1. Prepare each source device in the device group.
2. Create and save an archive for each device.
3. Download an archive file for each device.
4. Force source device 1 offline, and observe that source device 2 becomes active.
5. Shut down source device 1.
6. Install target device 1.
7. Prepare target device 1.
8. Upload the source device 1 archive, and load the archive onto the target device 1.

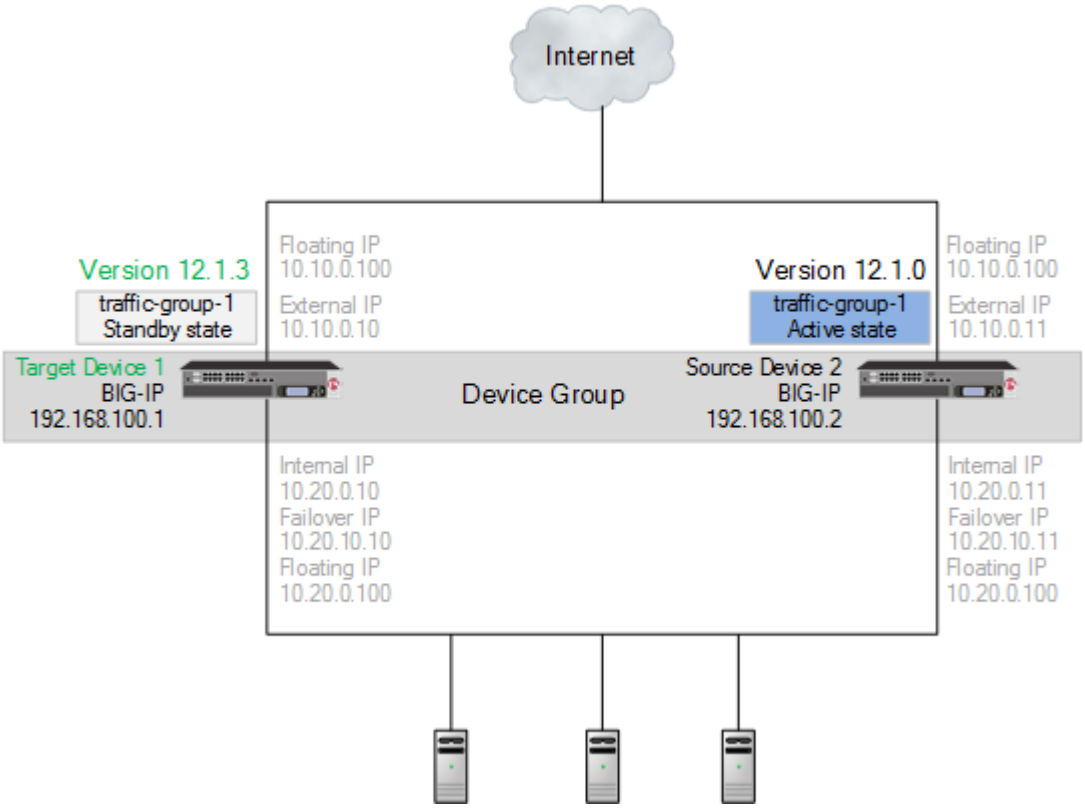

Figure 2: Migrated target device 1 in a device group

Step 2. Migrate source device 2 to target device 2.

1. Force source device 2 offline, and observe that target device 1 becomes active.
2. Shut down source device 2.
3. Install target device 2.
4. Prepare target device 2.
5. Upload the source device 2 archive, and load the archive onto the target device 2, reestablishing the device group.

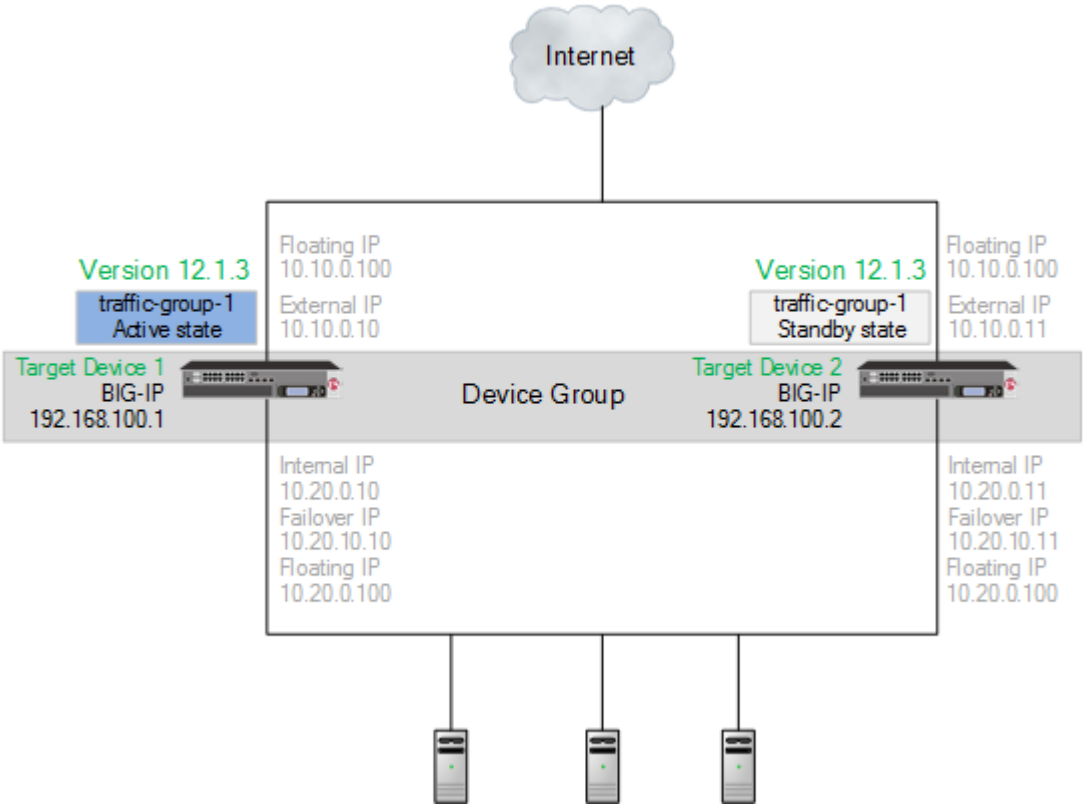

Figure 3: Migrated target device 1 and target device 2 in a device group

About migrating to a target device

You can easily take an existing configuration on a source device (appliance, VIPRION®, VE, or vCMP® guest) and replicate it on a target device (appliance, VIPRION, VE, or vCMP guest). The migration process includes the following steps:

1. Prepare the source device
2. Archive and download the UCS file
3. Shut down the source device
4. Set up the target device
5. Upload the archived UCS file
6. Load the archived UCS file onto the target device

For a device group, the migration functionality reestablishes the device group with the target devices when you load an archive onto the second target device.

Task Summary

Preparing BIG-IP modules for an upgrade from version 11.x, or later
Preparing RAID drives for an upgrade
Preparing a source device
Creating and saving an archive using the Configuration utility
Downloading a copy of an archive to a management workstation
Shutting down a source device
Installing a target device
Preparing a target device for migration

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

Feature or Functionality	Description
	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 a source device

You can use these steps to prepare a source device for migration to a target device.

1. Open the Traffic Management Shell (`tmsh`).
   ```
   tmsh
   ```
   This starts `tmsh` in interactive shell mode, and displays the `tmsh` prompt: `(tmos)#`.
2. Set the device master key to prompt for a password.
   ```
   (tmos)# modify sys crypto master-key prompt-for-password
   ```

   Tip: *This master key password is used when configuring the source and target devices. You will want to remember or safely record it for configuration of source and target devices.*

3. Enter a password.
   ```
   enter password: type_password
   ```
4. Confirm the password.
   ```
   password again: type_password
   ```
5. On the Main tab, click **Device Management** > **Overview**.

   In the Devices area of the screen, in the Sync Status column, view the sync status of each device:

- If all devices show a sync status of green, the configurations of all device members are synchronized, and you do not need to perform a config sync operation.
- If any device shows a sync status of Changes Pending, you must synchronize the configuration on that device to the other members of the device group.

A status of `Changes Pending` for a device indicates that the device contains recent configuration changes that have not yet been synchronized to the other members of the device group.

6. For each device, sync the configuration:
   a) On the Main tab, click **Device Management** > **Overview**.
   b) In the Device Groups area of the screen, in the Name column, select the name of the relevant device group.
      The screen expands to show a summary and details of the sync status of the selected device group, as well as a list of the individual devices within the device group.
   c) In the Devices area of the screen, in the Sync Status column, select a device.
   d) From the **Sync** options list, select a sync option.

Option	Description
Sync Device to Group	Select this option to synchronize the configuration of the selected device to the device group.
Sync Group to Device	Select this option to synchronize the configuration of the device group to the selected device.

   e) Click **Sync**.

The source device is prepared for migration to a target device

Creating and saving an archive using the Configuration utility

You can use the BIG-IP® Configuration utility to create and save archives on the BIG-IP system.

Important: *Any UCS file that you create includes the host name of the BIG-IP system as part of the data stored in that file. Later, when you specify this UCS file while restoring configuration data to a BIG-IP system, the host name stored in this UCS file must match the host name of the system to which you are restoring the configuration data. Otherwise, the system does not fully restore the data. Also, if your configuration data includes SSL keys and certificates, make sure to store the archive file in a secure environment.*

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

      Important: *Once the source device changes to the 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. On the Main tab, click **System** > **Archives**.
   The Archives screen displays a list of existing UCS files.

3. Click **Create**.

*Note: If the **Create** button is unavailable, you do not have permission to create an archive. You must have the Administrator role assigned to your user account.*

4. In the **File Name** field, type a unique file name for the archive.

   F5® recommends that the file name match the name of the BIG-IP system. For example, if the name of the BIG-IP system is `bigip2`, then the name of the archive file should be `bigip2.ucs`.

5. To encrypt the archive, for the **Encryption** setting, select **Enabled**.

*Note: If the **Encryption** setting is unavailable, you must configure the **Archive Encryption** setting located on the Preferences screen.*

6. To include private keys, for the **Private Keys** setting, select **Include**.

   Make sure to store the archive file in a secure environment.

7. Click **Finished**.

Downloading a copy of an archive to a management workstation

You can use the Configuration utility to download a copy of an archive to a management workstation. This provides an extra level of protection by preserving the configuration data on a remote system. In the unlikely event that you need to restore the data, and a BIG-IP® system event prevents you from accessing the archive in the BIG-IP system directory, you still have a backup copy of the configuration data.

1. On the Main tab, click **System** > **Archives**.
   The Archives screen displays a list of existing UCS files.
2. In the File Name column, click the name of the archive that you want to view.

   This displays the properties of that archive.
3. For the **Archive File** setting, click the **Download: <filename>.ucs** button.
   A confirmation screen appears.
4. Click **Save**.

   The BIG-IP system downloads a copy of the UCS file to the system from which you initiated the download.

Shutting down a source device

Before you shut down a source device during the migration process, download a copy of the archive file to a management workstation.

You can shut down a BIG-IP® source device, as needed, when migrating a configuration to a new target device.

Complete one of these steps.

- For BIG-IP software version 11.x.x, type `halt`. When a message appears indicating that the device is halted, turn off the power.
- For BIG-IP software version 12.0.0, and later, type `shutdown`.

The BIG-IP source device is shut down.

Installing a target device

You can install a target device when migrating from an older source device to a new target device.

1. Install and license the new target device in accordance with the platform guide installation instructions for the device.

   Note: *When installing the new target device, use the Configuration utility to specify the same IP address, Netmask, and Management Route as the source device.*

2. Provision the target device according to the provisioning of the source device.

The target device is installed, licensed, and provisioned.

Preparing a target device for migration

You can prepare a target device for migration.

1. Open the Traffic Management Shell (`tmsh`).
   ```
   tmsh
   ```
   This starts `tmsh` in interactive shell mode, and displays the `tmsh` prompt: `(tmos)#`.
2. Set the device master key to prompt for a password.
   ```
   (tmos)# modify sys crypto master-key prompt-for-password
   ```

   Tip: *This master key password is used when configuring the source and target devices. You will want to remember or safely record it for configuration of source and target devices.*

3. Enter a password.
   ```
   enter password: type_password
   ```
4. Confirm the password.
   ```
   password again: type_password
   ```
5. Save the configuration.
   ```
   (tmos)# save sys config
   ```

The target device is prepared for migration.

Uploading an archive from a management workstation

If you previously downloaded a copy of an archive to a management workstation, you can upload that archive to the BIG-IP® system at any time. This is useful when a BIG-IP system event has occurred that has caused the archive stored on the BIG-IP system to either become unavailable or corrupted.

You can use the Configuration utility to upload a copy of an archive stored on a management workstation.

Note: *When you upload a copy of an archive, you must specify the exact path name for the directory in which the downloaded archive copy is stored.*

1. On the Main tab, click **System** > **Archives**.
   The Archives screen displays a list of existing UCS files.
2. Click **Upload**.
   The Upload screen opens.
3. For the **File Name** setting, click **Browse**.
4. For the **Options** setting, select the **Overwrite existing archive file** check box if you want the BIG-IP system to overwrite any existing archive file.

   Note: *The BIG-IP system overwrites an existing file with the uploaded file only when the name of the archive you are uploading matches the name of an archive on the BIG-IP system.*

5. Click **Upload**.
   The specified archive is now uploaded to the `/var/local/ucs` directory on the BIG-IP system.

Loading an archive using tmsh

Migration to newer devices running software version 12.1.3, or later, ignores the following configuration objects. If your configuration includes dependencies on any of these objects, you must reconfigure them on the new device before you load the UCS file onto that device.

Important: *You must reconfigure the following objects on the new target device to use the same names as the objects on the source device, before you load the UCS file onto that device*

- Interfaces
- Interface bundles
- Management IP address
- Management route

You can use `tmsh` to load and migrate data from an archive file. The `/var/local/ucs` directory is the only location on the BIG-IP® system from which you can migrate an archive. If no archive exists in that directory, then you cannot migrate configuration data.

Important: *The host name stored in the archive file must match the host name of the target BIG-IP device; otherwise, the system does not fully migrate the data.*

1. Open the Traffic Management Shell (`tmsh`).
   ```
   tmsh
   ```
   This starts `tmsh` in interactive shell mode, and displays the `tmsh` prompt: `(tmos)#`.
2. Load the configuration contained in a specified UCS file.

   ```
   (tmos)# load sys ucs my_file.ucs platform-migrate
   ```

   Note: *When you load the configuration for a second device in a device group, the migration functionality reestablishes the device group.*

   The UCS is loaded into the running configuration of the device.

The archive file is loaded onto the target device.

Migration of Devices Running the Same Software Version

About migrating devices running the same software version

What is device migration?

Device migration enables you to replace the devices in a BIG-IP® device group running software version 12.1.3, or later, with newer devices running the same software version. It enables you to take an existing configuration on a device group's source device and easily replicate it on a target device.

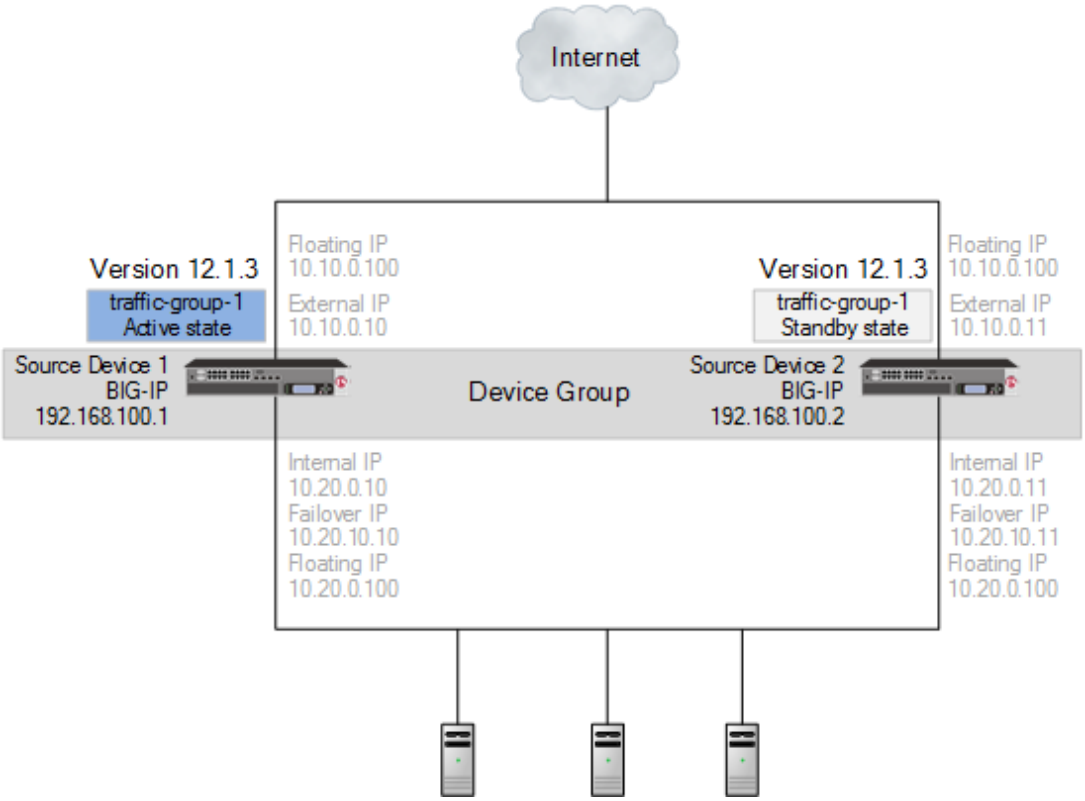

Figure 4: Source devices in a device group

Supported platforms

Supported source and target platforms include appliances, VIPRION® platforms, virtual edition (VE) devices, and vCMP® guests.

Configuration Dependencies

Migration to newer devices running software version 12.1.3, or later, ignores the following configuration objects. If your configuration includes dependencies on any of these objects, you must reconfigure them on the new device before you load the UCS file onto that device.

Important: *You must reconfigure the following objects on the new target device to use the same names as the objects on the source device, before you load the UCS file onto that device*

- Interfaces

- Interface bundles
- Management IP address
- Management route

Migration of a device group running the same software version

When you migrate the source devices in a device group running BIG-IP® software version 12.1.3, or later, to new target devices running the same BIG-IP software version, the following sequence of steps applies. This sequence migrates a device group composed of source devices 1 and 2 to a device group composed of new target devices 1 and 2.

Important:

- For a device group, migration functionality reestablishes the device group with the target devices when you load an archive onto the second target device.
- During migration, do not make any additional configuration changes. Reconfiguration during migration can cause unexpected behavior.
- Devices run different software versions during migration, preventing normal config sync functionality until migration completes.

Step 1. Migrate source device 1 to target device 1.

1. Prepare each source device in the device group.
2. Create and save an archive for each device.
3. Download an archive file for each device.
4. Force source device 1 offline, and observe that source device 2 becomes active.
5. Shut down source device 1.
6. Install target device 1.
7. Prepare target device 1.
8. Upload the source device 1 archive, and load the archive onto the target device 1.

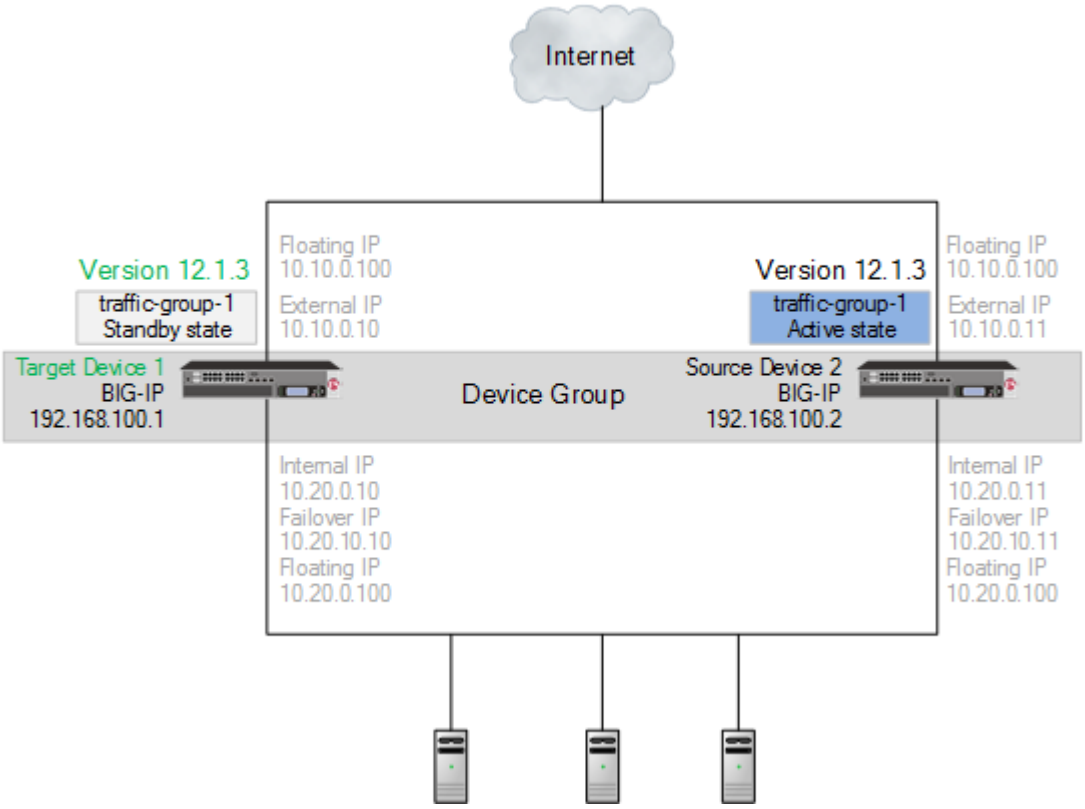

Figure 5: Migrated target device 1 in a device group

Step 2. Migrate source device 2 to target device 2.

1. Force source device 2 offline, and observe that target device 1 becomes active.
2. Shut down source device 2.
3. Install target device 2.
4. Prepare target device 2.
5. Upload the source device 2 archive, and load the archive onto the target device 2, reestablishing the device group.

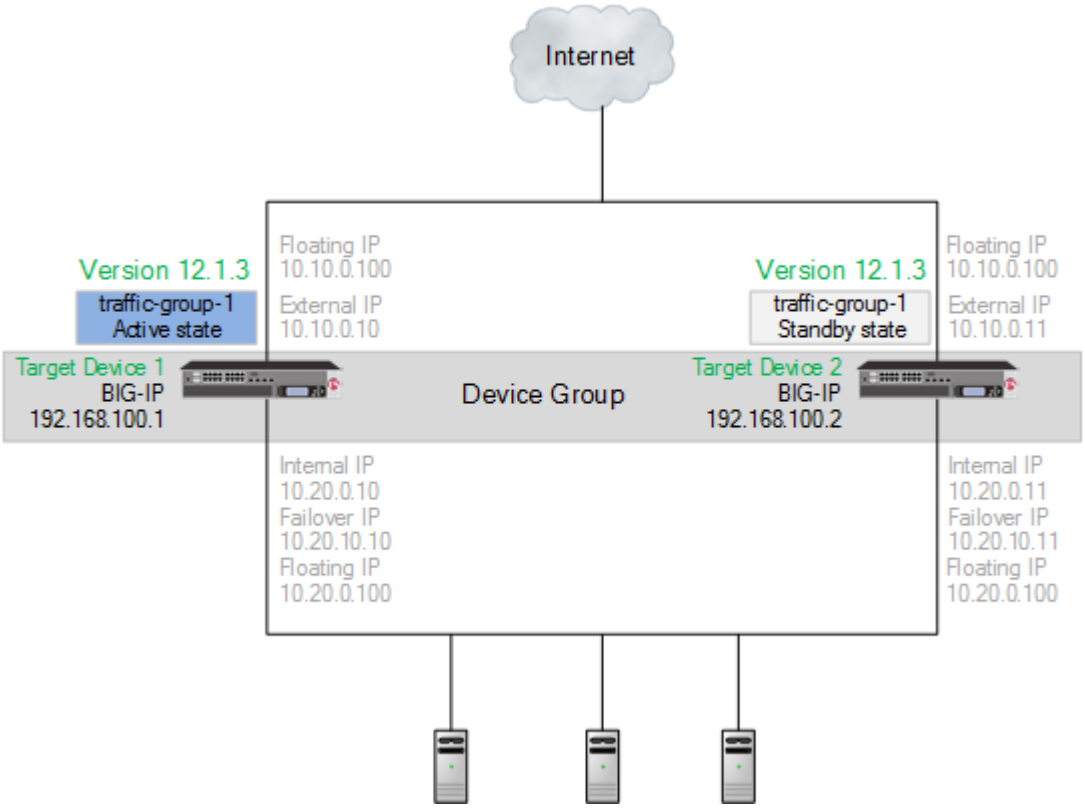

Figure 6: Migrated target device 1 and target device 2 in a device group

About migrating to a target device

You can easily take an existing configuration on a source device (appliance, VIPRION®, VE, or vCMP® guest) and replicate it on a target device (appliance, VIPRION, VE, or vCMP guest). The migration process includes the following steps:

1. Prepare the source device
2. Archive and download the UCS file
3. Shut down the source device
4. Set up the target device
5. Upload the archived UCS file
6. Load the archived UCS file onto the target device

For a device group, the migration functionality reestablishes the device group with the target devices when you load an archive onto the second target device.

Task Summary

Preparing a source device
Creating and saving an archive using the Configuration utility
Downloading a copy of an archive to a management workstation
Shutting down a source device
Installing a target device
Preparing a target device for migration
Uploading an archive from a management workstation
Loading an archive using tmsh

Preparing a source device

You can use these steps to prepare a source device for migration to a target device.

1. Open the Traffic Management Shell (`tmsh`).
   ```
   tmsh
   ```
   This starts `tmsh` in interactive shell mode, and displays the `tmsh` prompt: `(tmos)#`.
2. Set the device master key to prompt for a password.
   ```
   (tmos)# modify sys crypto master-key prompt-for-password
   ```

   Tip: *This master key password is used when configuring the source and target devices. You will want to remember or safely record it for configuration of source and target devices.*

3. On the Main tab, click **Device Management** > **Overview**.

   In the Devices area of the screen, in the Sync Status column, view the sync status of each device:

   - If all devices show a sync status of green, the configurations of all device members are synchronized, and you do not need to perform a config sync operation.
   - If any device shows a sync status of Changes Pending, you must synchronize the configuration on that device to the other members of the device group.

   A status of `Changes Pending` for a device indicates that the device contains recent configuration changes that have not yet been synchronized to the other members of the device group.
4. For each device, sync the configuration:
   a) On the Main tab, click **Device Management** > **Overview**.
   b) In the Device Groups area of the screen, in the Name column, select the name of the relevant device group.
      The screen expands to show a summary and details of the sync status of the selected device group, as well as a list of the individual devices within the device group.
   c) In the Devices area of the screen, in the Sync Status column, select a device.
   d) From the **Sync** options list, select a sync option.

Option	Description
Sync Device to Group	Select this option to synchronize the configuration of the selected device to the device group.
Sync Group to Device	Select this option to synchronize the configuration of the device group to the selected device.

   e) Click **Sync**.

The source device is prepared for migration to a target device

Creating and saving an archive using the Configuration utility

You can use the BIG-IP® Configuration utility to create and save archives on the BIG-IP system.

Important: *Any UCS file that you create includes the host name of the BIG-IP system as part of the data stored in that file. Later, when you specify this UCS file while restoring configuration data to a BIG-IP system, the host name stored in this UCS file must match the host name of the system to which you are restoring the configuration data. Otherwise, the system does not fully restore the data. Also, if your configuration data includes SSL keys and certificates, make sure to store the archive file in a secure environment.*

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

   Important: *Once the source device changes to the 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. On the Main tab, click **System** > **Archives**.
   The Archives screen displays a list of existing UCS files.
3. Click **Create**.

   Note: *If the* ***Create*** *button is unavailable, you do not have permission to create an archive. You must have the Administrator role assigned to your user account.*
4. In the **File Name** field, type a unique file name for the archive.
   F5® recommends that the file name match the name of the BIG-IP system. For example, if the name of the BIG-IP system is `bigip2`, then the name of the archive file should be `bigip2.ucs`.
5. To encrypt the archive, for the **Encryption** setting, select **Enabled**.

   Note: *If the* ***Encryption*** *setting is unavailable, you must configure the* ***Archive Encryption*** *setting located on the Preferences screen.*
6. To include private keys, for the **Private Keys** setting, select **Include**.
   Make sure to store the archive file in a secure environment.
7. Click **Finished**.

Downloading a copy of an archive to a management workstation

You can use the Configuration utility to download a copy of an archive to a management workstation. This provides an extra level of protection by preserving the configuration data on a remote system. In the unlikely event that you need to restore the data, and a BIG-IP® system event prevents you from accessing the archive in the BIG-IP system directory, you still have a backup copy of the configuration data.

1. On the Main tab, click **System** > **Archives**.
   The Archives screen displays a list of existing UCS files.
2. In the File Name column, click the name of the archive that you want to view.
   This displays the properties of that archive.
3. For the **Archive File** setting, click the **Download: <filename>.ucs** button.
   A confirmation screen appears.
4. Click **Save**.
   The BIG-IP system downloads a copy of the UCS file to the system from which you initiated the download.

Shutting down a source device

Before you shut down a source device during the migration process, download a copy of the archive file to a management workstation.

You can shut down a BIG-IP® source device, as needed, when migrating a configuration to a new target device.

Complete one of these steps.

- For BIG-IP software version 11.x.x, type `halt`. When a message appears indicating that the device is halted, turn off the power.
- For BIG-IP software version 12.0.0, and later, type `shutdown`.

The BIG-IP source device is shut down.

Installing a target device

You can install a target device when migrating from an older source device to a new target device.

1. Install and license the new target device in accordance with the platform guide installation instructions for the device.

   Note: *When installing the new target device, use the Configuration utility to specify the same IP address, Netmask, and Management Route as the source device.*

2. Provision the target device according to the provisioning of the source device.

The target device is installed, licensed, and provisioned.

Preparing a target device for migration

You can prepare a target device for migration.

1. Open the Traffic Management Shell (`tmsh`).
   ```
   tmsh
   ```
   This starts `tmsh` in interactive shell mode, and displays the `tmsh` prompt: `(tmos)#`.
2. Set the device master key to prompt for a password.
   ```
   (tmos)# modify sys crypto master-key prompt-for-password
   ```

   Tip: *This master key password is used when configuring the source and target devices. You will want to remember or safely record it for configuration of source and target devices.*

3. Save the configuration.
   ```
   (tmos)# save sys config
   ```

The target device is prepared for migration.

Uploading an archive from a management workstation

If you previously downloaded a copy of an archive to a management workstation, you can upload that archive to the BIG-IP® system at any time. This is useful when a BIG-IP system event has occurred that has caused the archive stored on the BIG-IP system to either become unavailable or corrupted.

You can use the Configuration utility to upload a copy of an archive stored on a management workstation.

Note: *When you upload a copy of an archive, you must specify the exact path name for the directory in which the downloaded archive copy is stored.*

1. On the Main tab, click **System** > **Archives**.
   The Archives screen displays a list of existing UCS files.
2. Click **Upload**.

The Upload screen opens.

3. For the **File Name** setting, click **Browse**.
4. For the **Options** setting, select the **Overwrite existing archive file** check box if you want the BIG-IP system to overwrite any existing archive file.

   Note: *The BIG-IP system overwrites an existing file with the uploaded file only when the name of the archive you are uploading matches the name of an archive on the BIG-IP system.*

5. Click **Upload**.
   The specified archive is now uploaded to the `/var/local/ucs` directory on the BIG-IP system.

Loading an archive using tmsh

Migration to newer devices running software version 12.1.3, or later, ignores the following configuration objects. If your configuration includes dependencies on any of these objects, you must reconfigure them on the new device before you load the UCS file onto that device.

Important: *You must reconfigure the following objects on the new target device to use the same names as the objects on the source device, before you load the UCS file onto that device*

- Interfaces
- Interface bundles
- Management IP address
- Management route

You can use `tmsh` to load and migrate data from an archive file. The `/var/local/ucs` directory is the only location on the BIG-IP® system from which you can migrate an archive. If no archive exists in that directory, then you cannot migrate configuration data.

Important: *The host name stored in the archive file must match the host name of the target BIG-IP device; otherwise, the system does not fully migrate the data.*

1. Open the Traffic Management Shell (`tmsh`).
   ```
   tmsh
   ```
   This starts `tmsh` in interactive shell mode, and displays the `tmsh` prompt: `(tmos)#`.
2. Load the configuration contained in a specified UCS file.

   ```
   (tmos)# load sys ucs my_file.ucs platform-migrate
   ```

   Note: *When you load the configuration for a second device in a device group, the migration functionality reestablishes the device group.*

   The UCS is loaded into the running configuration of the device.

The archive file is loaded onto the target device.

Legal Notices

Legal notices

Publication Date

This document was published on December 4, 2017.

Publication Number

MAN-0639-01

Copyright

Trademarks

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

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

Patents

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

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.

Legal Notices

Index