# F5® BIG-IQ® Centralized Management: Upgrading Logging Nodes to Version 5.2 While Preserving Existing Data

Version 5.2

# Table of Contents

# Logging Node Upgrade Overview (with Data)

## Which upgrade workflow should I use?

There are two workflows you can follow to upgrade BIG-IQ® Centralized Management Logging Node cluster. Before you start the upgrade process, decide which workflow is appropriate for you.

- To preserve the data collected with the current version of BIG-IQ Logging Node, use the work flow in this guide (BIG-IQ® Centralized Management: Upgrading Logging Nodes to Version 5.2 While Preserving Existing Data.
- If you just want to upgrade, and do not care about your data, use *F5® BIG-IQ® Centralized Management: Upgrading Logging Nodes to Version 5.2 Without Preserving Existing Data*

## How do I upgrade my Logging Node cluster to version 5.2 and preserve my existing data?

A *Logging Node cluster* is made up of all of your Logging Nodes, the BIG-IQ® Centralized Management device you use to manage them, and any BIG-IQ peer devices. If you use a Logging Node cluster to store and manage your alerts and events, there are additional steps in the upgrade process.

---

***Important:*** *Upgrading the Logging Node cluster requires taking the cluster offline. To prevent losing alerts and event log data, you must perform this process during a maintenance window.*

---

---

***Important:*** *In version 5.2, the name of the device referred to in version 5.1 as a "Logging Node" is changed. As the diagram shows, after the upgrade, the device is referred to as a "Data Collection Device" or DCD.*

---

The diagram illustrates the process workflow:

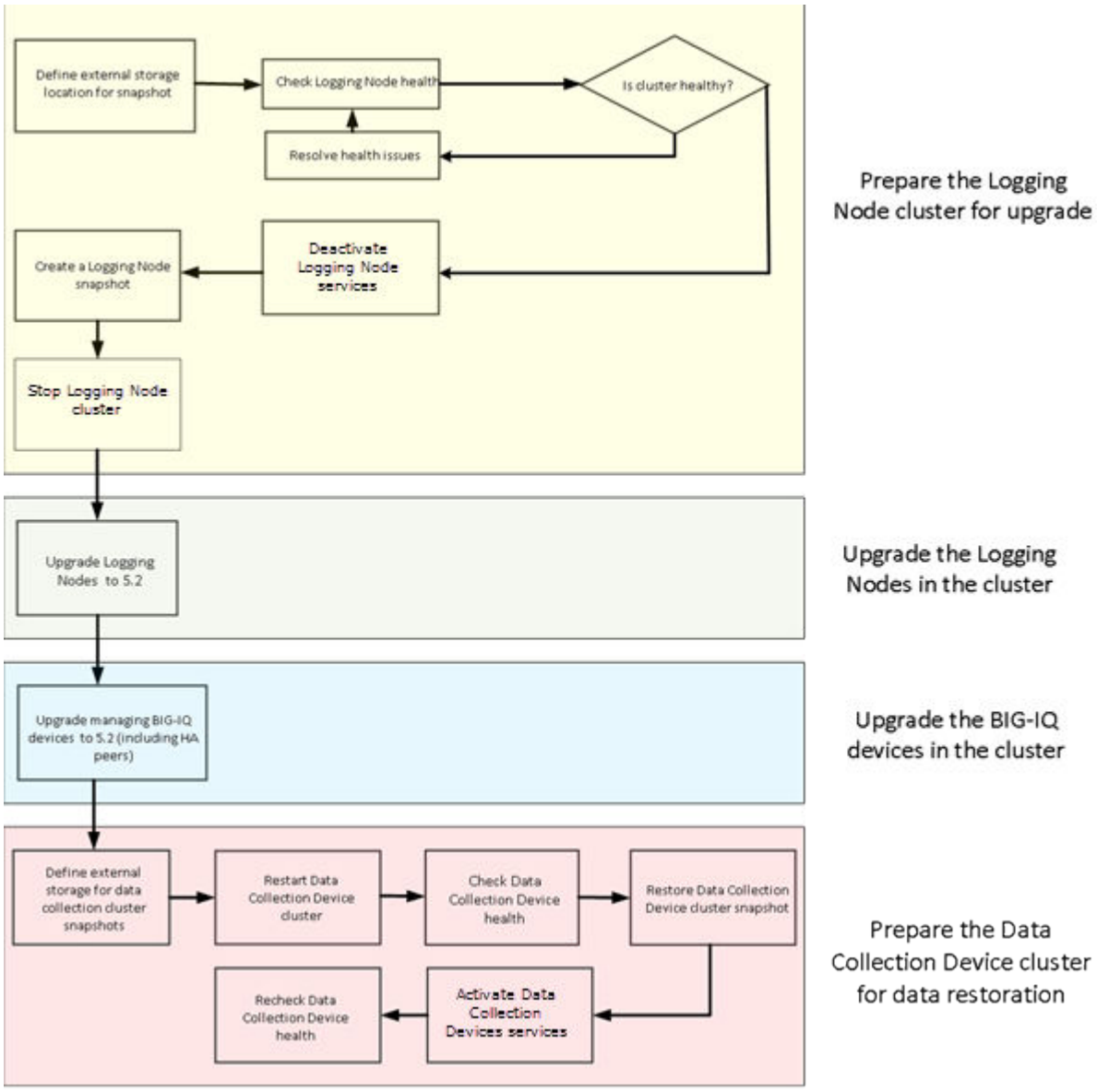



**Figure 1: Logging Node upgrade worfklow**

***Note:*** *For a successful upgrade, it is essential that you perform the tasks in the sequence detailed here. You cannot perform these tasks in parallel.*

## Logging Node cluster update requirements

There are a number of items that you need to have ready access to, before you can successfully complete the Logging Node cluster update. It might be helpful to use the following table to record the values so you have them at hand when needed.

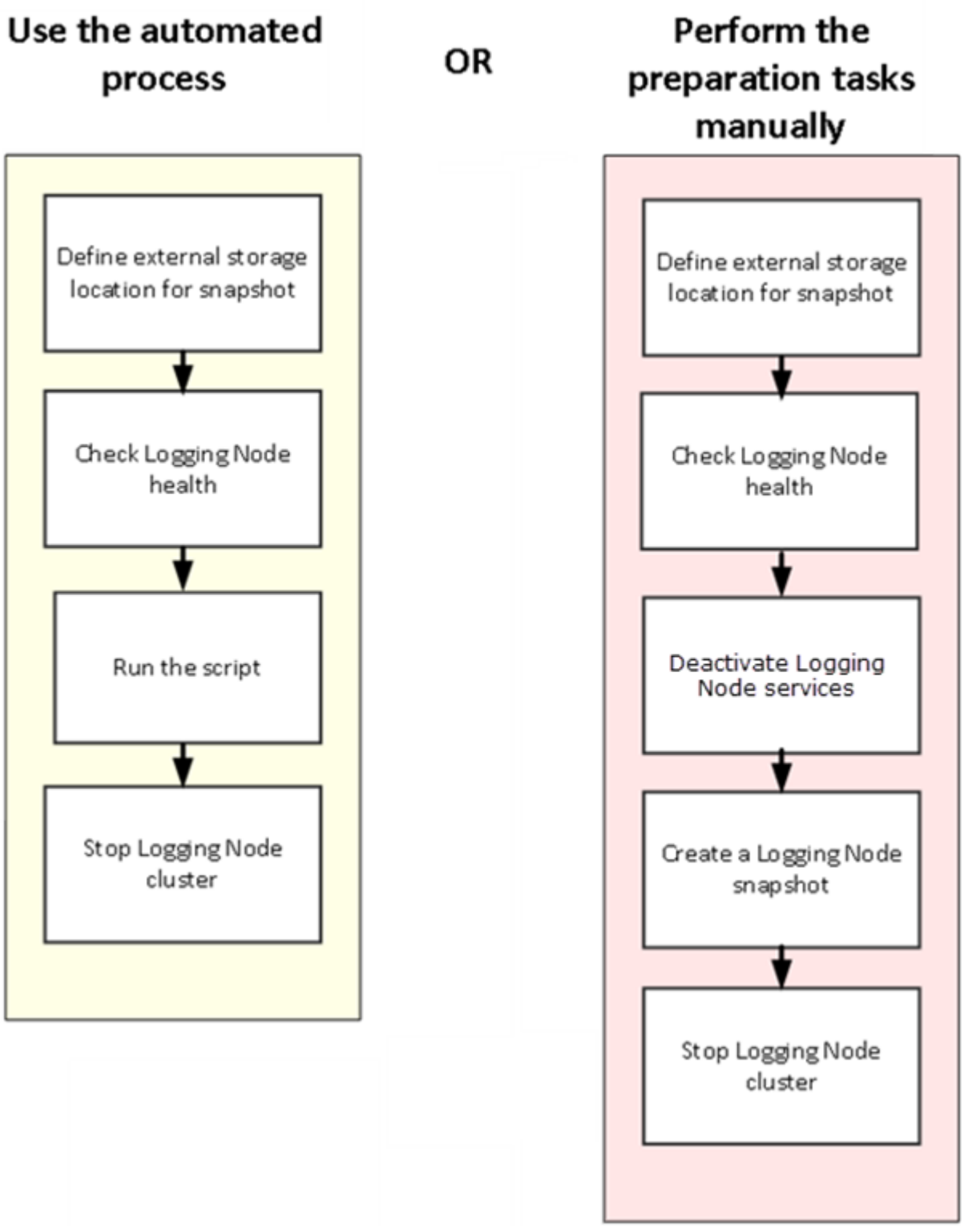
| Device | Information needed | Information Recorded |
|---|---|---|
| Primary BIG-IQ Centralized Management device | Management IP address<br>admin user name and password | |

| Device | Information needed | Information Recorded |
|---|---|---|
| | root access password | |
| Secondary BIG-IQ device | Management IP address | |
| | root access password | |
| Logging Nodes | Management IP address | |
| | root access password | |
| Storage Machine | IP-address | |
| | storage file path | |
| | Read/Write permissions for the storage file path | |
| | root access password | |
| All devices | To successfully complete some of the procedures in the upgrade process, rudimentary knowledge of Linux commands is very helpful. | |

## Logging Node preparation options

Before you start the upgrade, there are a few tasks to do. To make sure that this process goes smoothly, F5 provides a script that automates the preparation process. You can either run this script, or perform the preparation tasks yourself.

The diagram illustrates these two work flows, automated on the left:


Use the automated process
OR
Perform the preparation tasks manually
Define external storage location for snapshot
Check Logging Node health
Run the script
Stop Logging Node cluster
Define external storage location for snapshot
Check Logging Node health
Deactivate Logging Node services
Create a Logging Node snapshot
Stop Logging Node cluster

# Prepare for Logging Node Upgrade (automated)

## Prepare the Logging Node cluster for upgrade (automated method)

If you choose this automated method, you prepare for the upgrade using a script. This script stops Logging Node services on all devices in the cluster, and creates a snapshot that preserves your existing Logging Node data. This method makes it much more likely that the upgrade process goes smoothly.

### Define external storage snapshot locations

Before you can configure the external snapshot storage location, you need the following information on the machine you will use to store the snapshots:

- Storage-machine-IP-address
- Storage-file-path
- User name, password, and (optionally) the domain for the storage file path
- Read/Write permissions for the storage file path

You need snapshots so you can restore the Logging Node data, especially after performing software upgrades.

When snapshots are created, they need to be stored on a machine other than the Logging Node that stores the data. You define the location for the snapshot by editing the `fstab` file on each device in your Logging Node cluster.

---

***Important:*** *You must perform this task on each Logging Node device, on the BIG-IQ® Centralized Management device, and on the BIG-IQ HA peer.*

---

1. On the device, in the folder `/var/config/rest/elasticsearch/data/`, create a new folder named `essnapshot`.
   `mkdir /var/config/rest/elasticsearch/data/essnapshot`
2. Edit the `/etc/fstab` file.
   - If there is a valid domain available, add the following entry: `//<storage machine ip-address>/<storage-filepath> /var/config/rest/elasticsearch/data/essnapshot cifs iocharset=utf8,rw,noauto,uid=elasticsearch,gid=elasticsearch,user=<username>,domain=<domain name> 0 0`
   - If there is no valid domain available, add the following entry: `//<storage machine ip-address>/<storage-filepath> /var/config/rest/elasticsearch/data/essnapshot cifs iocharset=utf8,rw,noauto,uid=elasticsearch,gid=elasticsearch,user=<username> 0 0`
3. Run the following command sequence to mount the snapshot storage location to the `essnapshot` folder. Type the password when prompted.
   - `# cd /var/config/rest/elasticsearch/data`
   - `# mount essnapshot`
   - `Password:`
4. Confirm that the `essnapshot` folder has full read, write, and execute permissions, (specifically `chmod 777 essnapshot`), and that the owner and group are `elasticsearch` for this folder.

For example, `ls-l` yields: `drwxrwxrwx 3 elasticsearch elasticsearch 0 Apr 25 11:27 essnapshot`.

5. Create a test file to confirm that the storage file path has been successfully mounted.
   For example: `touch testfile`.
   The test file should be created on the storage machine at the location storage file path.
6. Repeat these five steps for each Logging Node, the BIG-IQ Centralized Management, and the BIG-IQ HA peer device.

The storage location should now be accessible to all of the devices in the Logging Node cluster.

## Check Logging Node health

You can use the Logging Configuration screen to review the overall health and status of the Logging Nodes you've configured. You can use the data displayed on this screen both before and after an upgrade to verify that your Logging Node cluster configuration is as you expect it to be.

---

***Note:*** *Perform this check on the BIG-IQ® Centralized Management device; not on the Logging Node.*

---

1. At the top of the screen, click **System Management**.
2. At the top of the screen, click **Inventory**.
3. On the left, expand **BIG-IQ LOGGING** and then select **Logging Configuration**.
   The Logging Configuration screen opens to display the current state of the logging node cluster defined for this device.
4. Record these Logging Node cluster details as listed in the Summary area.
   - Logging Nodes in Cluster
   - Nodes in Cluster
   - Total Document Count
   - Total Document Size

   This information provides a fairly detailed overview that describes the Logging Node cluster you have created to store alert or event data. After you complete an upgrade, you can check the health again, and use this information to verify that the cluster restored successfully.
5. If there are any cluster health issues, resolve those issues and then repeat the process until the cluster health is as expected.

## Run the upgrade preparation script

Running the upgrade preparation script is the safest way to prepare for the Logging Node upgrade. Using the automated script eliminates the chance of either omitting a step, or typing in an incorrect value, either of which could lead to failure for the entire upgrade process.

1. Use SSH to log in to the BIG-IQ Centralized Management device.
2. Run the script file, and respond to the username and password prompts with the admin user name and password.

   ---

   ***Note:*** *The script file resides in the `/usr/bin/` folder on the BIG-IQ Centralized Management device.*

   ---

   ```
   /usr/bin/upgradeprep.sh
   ```

When the script completes, you should see the line: `Snapshot taken successfully`, followed by the name of the snapshot it created. Depending on your security configuration, this line may not be the very last line that displays in the system output, but it should be easy to spot.

Once the script runs successfully, you can proceed with the next step: *Stop Logging Node cluster*.

## Stop Logging Node cluster

As part of preparing to upgrade your Logging Node, you must shut down the cluster so that upgraded devices and devices that have not yet upgraded do not communicate during the upgrade.

***Important:*** *If you omit this step, the cluster will not function after the upgrade.*

***Note:*** *You must perform this task on each device in the cluster (that is, each Logging Node device, the BIG-IQ® Centralized Management device, and the BIG-IQ HA peer).*

1. Use SSH to log in to a device in the cluster.

   You must log in as `root` to perform this procedure.
2. Run the following command to stop the cluster on this device:
   ```
   bigstart stop elasticsearch
   ```
3. Run the following command to confirm that the cluster is stopped on this device:
   ```
   bigstart status elasticsearch
   ```
4. Repeat the last three steps for each device in the cluster.

Once you have stopped the cluster for each device, you can proceed with the cluster upgrade.

# Prepare for Logging Node Upgrade (manual)

## Prepare the Logging Node cluster for upgrade (manual method)

If you choose this method, you perform the upgrade without using a script. This method requires a little more attention to detail on your part to ensure that the upgrade process goes smoothly.

### Define external storage snapshot locations

Before you can configure the external snapshot storage location, you need the following information on the machine you will use to store the snapshots:

- Storage-machine-IP-address
- Storage-file-path
- User name, password, and (optionally) the domain for the storage file path
- Read/Write permissions for the storage file path

You need snapshots so you can restore the Logging Node data, especially after performing software upgrades.

When snapshots are created, they need to be stored on a machine other than the Logging Node that stores the data. You define the location for the snapshot by editing the `fstab` file on each device in your Logging Node cluster.

---

***Important:*** *You must perform this task on each Logging Node device, on the BIG-IQ® Centralized Management device, and on the BIG-IQ HA peer.*

---

1. On the device, in the folder `/var/config/rest/elasticsearch/data/`, create a new folder named `essnapshot`.
   `mkdir /var/config/rest/elasticsearch/data/essnapshot`
2. Edit the `/etc/fstab` file.
   - If there is a valid domain available, add the following entry: `//<storage machine ip-address>/<storage-filepath> /var/config/rest/elasticsearch/data/essnapshot cifs iocharset=utf8,rw,noauto,uid=elasticsearch,gid=elasticsearch,user=<username>,domain=<domain name> 0 0`
   - If there is no valid domain available, add the following entry: `//<storage machine ip-address>/<storage-filepath> /var/config/rest/elasticsearch/data/essnapshot cifs iocharset=utf8,rw,noauto,uid=elasticsearch,gid=elasticsearch,user=<username> 0 0`
3. Run the following command sequence to mount the snapshot storage location to the `essnapshot` folder. Type the password when prompted.
   - `# cd /var/config/rest/elasticsearch/data`
   - `# mount essnapshot`
   - `Password:`
4. Confirm that the `essnapshot` folder has full read, write, and execute permissions, (specifically `chmod 777 essnapshot`), and that the owner and group are `elasticsearch` for this folder. For example, `ls-l` yields: `drwxrwxrwx 3 elasticsearch elasticsearch 0 Apr 25 11:27 essnapshot`.

5. Create a test file to confirm that the storage file path has been successfully mounted.
   For example: `touch testfile`.
   The test file should be created on the storage machine at the location storage file path.
6. Repeat these five steps for each Logging Node, the BIG-IQ Centralized Management, and the BIG-IQ HA peer device.

The storage location should now be accessible to all of the devices in the Logging Node cluster.

## Check Logging Node health

You can use the Logging Configuration screen to review the overall health and status of the Logging Nodes you've configured. You can use the data displayed on this screen both before and after an upgrade to verify that your Logging Node cluster configuration is as you expect it to be.

***Note:*** *Perform this check on the BIG-IQ® Centralized Management device; not on the Logging Node.*

1. At the top of the screen, click **System Management**.
2. At the top of the screen, click **Inventory**.
3. On the left, expand **BIG-IQ LOGGING** and then select **Logging Configuration**.
   The Logging Configuration screen opens to display the current state of the logging node cluster defined for this device.
4. Record these Logging Node cluster details as listed in the Summary area.
   - Logging Nodes in Cluster
   - Nodes in Cluster
   - Total Document Count
   - Total Document Size

   This information provides a fairly detailed overview that describes the Logging Node cluster you have created to store alert or event data. After you complete an upgrade, you can check the health again, and use this information to verify that the cluster restored successfully.
5. If there are any cluster health issues, resolve those issues and then repeat the process until the cluster health is as expected.

## Deactivate Logging Node services

Before you can successfully upgrade your Logging Node cluster, you must deactivate the services that send alerts or events to the Logging Nodes.

***Note:*** *Perform this check on the BIG-IQ® Centralized Management device; not on the Logging Node.*

1. At the top of the screen, click **System Management**.
2. On the left, expand **BIG-IQ LOGGING** and then select **Logging Nodes**.
3. Click the name of a Logging Node.
   The Properties screen for the selected device opens.
4. On the left, click **Services**.
5. For each active service, click **Deactivate**.
6. Click **Close**.
7. Repeat the steps for each Logging Node in the cluster.

The services on your Logging Nodes stop. Consequently, the Logging Nodes stop accepting alerts or events from the BIG-IP®.

## Create a Logging Node snapshot

Snapshots of the event logs sent to your Logging Nodes are an essential safeguard for your data. If the machine that stores the event logs fails, you can use these snapshots to restore the data. You define schedules for creating these snapshots.

1. At the top of the screen, click **System Management**.
2. At the top of the screen, click **Inventory**.
3. On the left, expand **BIG-IQ LOGGING** and then select **Logging Configuration**.
   The Logging Configuration screen opens to display the current state of the logging node cluster defined for this device.
4. Next to **Snapshot Schedules**, click **Create**.
   The New Logging Snapshot screen opens.
5. For the **Snapshot Name Prefix**, type the string that you want to use to identify this snapshot.

   We recommend you choose a name that identifies the snapshot as the backup of your Logging Node data (for example `lg_backup`).
6. For **Snapshots to Keep**, select **1**.
7. For the **Schedule Type**, select **Days of the Week**.
8. For the **Days of the Week** select the current day of the week.
9. For the **Start Date**, select the current day and time.
10. Click **Save** to save the new schedule.

When you click **Save**, the snapshot is created.

When the **Snapshot Count** increments, and the **Last Snapshot/Time** updates to show the snapshot you created, you can proceed with the next step: *Stop Logging Node cluster*.

## Stop Logging Node cluster

As part of preparing to upgrade your Logging Node, you must shut down the cluster so that upgraded devices and devices that have not yet upgraded do not communicate during the upgrade.

***Important:*** *If you omit this step, the cluster will not function after the upgrade.*

***Note:*** *You must perform this task on each device in the cluster (that is, each Logging Node device, the BIG-IQ® Centralized Management device, and the BIG-IQ HA peer).*

1. Use SSH to log in to a device in the cluster.

   You must log in as `root` to perform this procedure.
2. Run the following command to stop the cluster on this device:
   ```
   bigstart stop elasticsearch
   ```
3. Run the following command to confirm that the cluster is stopped on this device:
   ```
   bigstart status elasticsearch
   ```
4. Repeat the last three steps for each device in the cluster.

Once you have stopped the cluster for each device, you can proceed with the cluster upgrade.

# Upgrade the Logging Nodes in Your Cluster

## Upgrade the Logging Nodes to version 5.2

After you prepare the Logging Node cluster for upgrade, use these procedures to upgrade the Logging Nodes in your cluster.

### What you need to do before you upgrade the Logging Node from version 5.x to 5.2

Before upgrading the F5® BIG-IQ® Centralized Management Logging Node, perform these tasks.

| Tasks | Additional information |
|---|---|
| Re-activate the BIG-IQ system license. | You must do this on both the active and the secondary BIG-IQ if they are running in an HA pair. For specific instructions about how to reactivate a license, refer to the *F5® BIG-IQ® Central Management: Licensing and Initial Setup* guide. |
| Decide which disk volume you want to install the upgrade on. You must have at least two volumes to upgrade BIG-IQ. | If you are running BIG-IQ Virtual Edition and you don't have two volumes, refer to: K1740617406: Using the tmsh utility to create a new software volume for installing a new image or hotfix on the BIG-IQ system at: *support.f5.com/csp/article/K17406* |

Gather the following information.

| Required information | For my configuration |
|---|---|
| You'll need to create a passphrase for the Master Key. The passphrase must contain:<br>• At least 16 characters<br>• Contain at least 1 capital letter<br>• Contain at least 1 lower case letter<br>• Contain at least 1 number<br>• Contain at least 1 special character<br>***Important:*** *You must use the same Master Key Passphrase for each BIG-IQ system in an HA pair and every device in a Logging Node cluster. The upgrade will complete without it, but the HA pair or Logging Node cluster will not function if the pass phrases don't match.* | |

### Download the BIG-IQ version 5.2 software image from F5 Networks

Downloading a software image from F5 Networks is the first step to making it available to install on the Logging Node.

1. Log in to the F5 Downloads site, `downloads.f5.com`.

2. Click the **Find a Download** button.
3. Click the name of the product line.
4. Click the product name, **Centralized Management**.
5. Click **V5.2.0**.
6. Read the End User Software License agreement and click the **I Accept** button if you agree with the terms.
7. Click the BIG-IQ version 5.2 `.iso` file name.
8. Click the name of the closest geographical location to you.
   The software image downloads to your local system

The software image is now available for you to upload to the Logging Node.

## Upload the BIG-IQ version 5.2 software image

Before you can upload the software image to your Logging Node, you must have first downloaded it from the F5 Downloads site.

You upload the BIG-IQ version 5.2 software image to your Logging Node to make it available for this upgrade.

1. At the top of the screen, click **System Management**.
2. At the top of the screen, click **Inventory**.
3. On the left, click **SOFTWARE MANAGEMENT** > **Available Images**.
4. Click the **Upload Image** button.
5. Click the **Choose File** button and navigate to the location to which you downloaded the image, and click the **Open** button to upload it to BIG-IQ.
6. Click the **Upload** button.

   The screen refreshes to display the progress of the upload.

When the image is done uploading, it shows in the Available Images list.

## Upgrade the Logging Node to version 5.2

The default size of the `/var` file system in a newly installed Logging Node is 10 GB. That may be insufficient to store logging data. Extending this file system to a larger size is explained in SOL 17406. Because upgrading a Logging Node installation requires at least two volumes, you must ensure that both volumes can have their `/var` file system extended to the same size, or upgrades may fail. If you are running BIG-IQ Virtual Edition and don't have two volumes, refer to: *SOL17406: Using the tmsh utility to create a new software volume for installing a new image or hotfix on the BIG-IQ system* at `support.f5.com/kb/en-us/solutions/public/17000/400/sol17406.html`

Before upgrading Logging Node, you must have downloaded the BIG-IQ version 5.2 `.iso` image from the F5 downloads site.

The upgrade process involves installing the new version of the software, booting into that new version, and reviewing the settings on the setup screens.

1. Log in to the Logging Node with your admin user name and password.
2. At the top of the screen, click **System Management**.
3. At the top of the screen, click **Inventory**.
4. On the left, click **BIG-IQ HA**.
5. Click the name of the Logging Node.
6. On the left, click **Software Version**.
7. Click the **Update** button.

8. From the **Software Image** list, select the image you want to install.
9. From the **Target Volume** list, select the volume you want to install the image on.
10. To prompt the Logging Node to reboot into the new software installation volume, select the **Reboot into Target Volume** check box.
11. Click the **Apply** button.
    A popup screen opens, prompting you to confirm the installation.
12. Click the **Continue** button.
13. Wait while the Logging Node loads the new software and reboots.

    Depending on your configuration and the number of devices you are managing, this could take up to 15 minutes. During this time, it is important that you not interrupt the installation process by restarting services or the server.
14. Log back in to the Logging Node.
15. If needed, extend the /var partition.

    The default size of the /var file system in a newly installed node is 10 GB. This volume size might be insufficient to store your data. You can see how to extend this file system to a larger size in knowledge article K16103. refer to: K16103: Extending disk space on BIG-IQ Virtual Edition at support.f5.com/csp/article/K16103. Because upgrading a node requires at least two volumes, you must ensure that both volumes can have their /var file system extended to the same size, or upgrades might fail.

---

***Important:*** *In the unlikely event that you are unable to log in to a BIG-IQ® 7000 series platform after you upgraded it, refer to SOL40338232: The BIG-IQ system interface might be inaccessible after the BIG-IQ system is upgraded from BIG-IQ Centralized Management version to 5.2.0 at* `support.f5.com/kb/en-us/solutions/public/k/40/sol40338232.html` *for more information.*

---

## After you upgrade to version 5.2

After you upgrade to BIG-IQ® version 5.2, you will notice a few differences in performance.

In BIG-IQ Logging, Logging Node, and logging configuration:

- In version 5.2, the Logging Node is referred to as a *data collection device*.
- When you configure the data collection device, you need to create a passphrase for the Master Key. You must use the same Master Key passphrase for each device in the data collection device cluster.

In Network Security:

- Web Application Security event logs created in a previous version of BIG-IQ are not compatible with BIG-IQ version 5.2.

# Upgrading BIG-IQ Centralized Management with Logging Nodes to Version 5.2

## What you need to do before you upgrade BIG-IQ from version 5.x to 5.2

Before upgrading F5® BIG-IQ® Centralized Management, perform the following tasks.

| Tasks | Additional information |
|---|---|
| Re-activate the BIG-IQ system license. | You must do this on both the active and the secondary BIG-IQ if they are running in an HA pair. For specific instructions about how to reactivate a license, refer to the *F5® BIG-IQ® Central Management: Licensing and Initial Setup* guide. |
| Create a backup of the BIG-IQ system's current compressed user configuration set (UCS) and store it on a remote server. | The UCS file includes: system-specific configuration files, license, user account and password information, and SSL certificates and keys. You can use this backup in the event you want to restore to the previous version of BIG-IQ. |
| Decide which disk volume you want to install the upgrade on. You must have at least two volumes to upgrade BIG-IQ. | If you are running BIG-IQ Virtual Edition and you don't have two volumes, refer to: K1740617406: Using the tmsh utility to create a new software volume for installing a new image or hotfix on the BIG-IQ system at: *support.f5.com/csp/article/K17406* |
| Deploy any staged configuration changes to your managed devices. | This step is required only if you are going to use the script to re-discover and re-import BIG-IP devices and services after the upgrade (as outlined in the section titled, *Re-discover devices and re-import services in bulk using a script*).<br>You must deploy configuration changes you have staged for your devices if you use this script, because they'll be overwritten on BIG-IQ after you run the script. If you'd rather re-discover devices and re-import services from the BIG-IQ user interface (instead of in bulk) so you can address any potential configuration conflicts for each BIG-IP device, refer to the section titled, *Re-discover devices and re-import services from the user interface*. |

Gather the following information:

| Required information | For my configuration |
|---|---|
| You'll need to create a passphrase for the Master Key. The passphrase must contain:<br>• At least 16 characters<br>• Contain at least 1 capital letter | |

| Required information | For my configuration |
|---|---|
| • Contain at least 1 lower case letter<br>• Contain at least 1 number<br>• Contain at least 1 special character<br><br>***Important:*** *You must use the same Master Key Passphrase for each BIG-IQ system in an HA pair and every device in a Logging Node cluster. The upgrade will complete without it, but the HA pair or Logging Node cluster will not function if the pass phrases don't match.* | |
| Get the discovery address you specified on the BIG-IQ system during setup. This is the same IP address that the peers in a high availability confirmation use to communicate. You can find this IP address on the BIG-IQ HA screen. | |
| Get your BIG-IQ administrator and root passwords. | |
| Get the name for the secondary HA BIG-IQ system if configured in an HA pair. | |

If you're currently running a version of BIG-IQ prior to version 5.0, you must first upgrade to version 5.0 before you can upgrade to version 5.2. For more information, refer to the guide titled, *F5 BIG-IQ Centralized Management: Upgrading BIG-IQ to Version 5.0*.

If you're upgrading BIG-IQ Logging Nodes, refer to the guide titled, *F5 BIG-IQ Centralized Management: Upgrading Logging Nodes to version 5.2*.

## Summary of procedures to upgrade BIG-IQ from version 5.x to 5.2

To upgrade F5® BIG-IQ® Centralized Management from BIG-IQ version 5.x to 5.2, perform these procedures. Upgrading BIG-IQ to the most recent version requires an update to its configuration to incorporate new features introduced. It's a good idea to set aside at least a few hours to complete this process.

***Note:*** *It is important that you follow these procedures in the order stated.*

1. Complete all of the pre-requisites outlined in the topic titled, *What you need to do before you upgrade BIG-IQ from version 5.x to 5.2*.
2. Download the BIG-IQ version 5.2 `iso` file from the F5 Downloads site to your desktop.
3. Upload the software image to the primary BIG-IQ system.
4. If configured in an HA pair:
   - Remove the secondary BIG-IQ system from the primary BIG-IQ system (if configured in an HA pair).
   - Upgrade the primary BIG-IQ system.
   - Upload the software image to the secondary BIG-IQ system.
   - Install the new software on the secondary BIG-IQ system.
   - Re-establish the HA configuration.
5. Upgrade the BIG-IP framework on your managed devices.

6. Re-discover devices and re-import LTM, ASM, AFT, and DNS services. Or, remove and recreate or reimport access groups for devices running APM services.

   ***Note:*** *You have the option to use a script from the command line to re-discover and re-import services (in bulk) for devices running LTM, ASM, AFM, and DNS or individually through the BIG-IQ user interface. For devices running the APM service, you must remove and recreate access groups for devices running the APM service. For more information, refer to, Use a script to remove and recreate access groups in bulk for devices running APM services,Remove and recreate access groups (with SWG data) from the user interface for devices running APM services or Reimport access groups (without SWG data) from the user interface for devices running APM services.*

## Download the BIG-IQ version 5.2 software image from F5 Networks

Downloading a software image from F5 Networks is the first step to making it available to install on the BIG-IQ system.

1. Log in to the F5 Downloads site, `downloads.f5.com`.
2. Click the **Find a Download** button.
3. Click the name of the product line.
4. Click the product name, **Centralized Management**.
5. Click **V5.2.0**.
6. Read the End User Software License agreement and click the **I Accept** button if you agree with the terms.
7. Click the BIG-IQ version 5.2 `.iso` file name.
8. Click the name of the closest geographical location to you.
   The software image downloads to your local system.

The software image is now available for you to upload.

## Upload the BIG-IQ version 5.2 software image

Before you can upload the software image to your BIG-IQ® system, you must have first downloaded it from the F5 Downloads site.

Upload the BIG-IQ version 5.2 software image to your BIG-IQ system to make it available for this upgrade.

1. At the top of the screen, click **System Management**.
2. At the top of the screen, click **Inventory**.
3. On the left, click **SOFTWARE MANAGEMENT** > **Available Images**.
4. Click the **Upload Image** button.
5. Click the **Choose File** button and navigate to the location to which you downloaded the image, and click the **Open** button to upload it to BIG-IQ.
6. Click the **Upload** button.

   The screen refreshes to display the progress of the upload.

When the image is done uploading, it shows in the Available Images list.

## Remove the secondary BIG-IQ from the HA pair

If the F5®BIG-IQ® Centralized Management system configured in an HA pair, you must remove the secondary BIG-IQ system before you upgrade the primary BIG-IQ.

1. Log in to the primary BIG-IQ system with your administrator user name and password.
2. At the top left of the screen, select **System Management** from the BIG-IQ menu.
3. At the top of the screen, click **Inventory**.
4. On the left, click **BIG-IQ HA**.
5. Select the check box next to the secondary BIG-IQ, and click the **Remove Device** button.
   A dialog box opens, prompting you to confirm that you want to remove the peer device from this group.
6. Click **Delete** in the dialog box to confirm the removal.

You can now upgrade the primary BIG-IQ.

## Upgrade the primary to BIG-IQ version 5.2

You need at least two volumes to upgrade F5® BIG-IQ® Centralized Management. If you are running BIG-IQ Virtual Edition and don't have two volumes, refer to: *K17406: Using the tmsh utility to create a new software volume for installing a new image or hotfix on the BIG-IQ system* at `support.f5.com/csp/article/K17406.html`

Before upgrading BIG-IQ, download the BIG-IQ version 5.2 `.iso` image from the F5 downloads site. Be sure to have your Master Key pass phrase handy; you'll need it after you reboot.

---

***Warning:*** *These procedures require that the BIG-IQ system is temporarily unavailable, and unable to manage BIG-IP® devices until the upgrade is complete. BIG-IP devices can continue to manage traffic during this time. This process can take up to an hour.*

---

Upgrade BIG-IQ to take advantage of the newest functionality and features..

1. Log in to the primary BIG-IQ with your admin user name and password.
2. At the top of the screen, click **System Management**.
3. At the top of the screen, click **Inventory**.
4. On the left, click **BIG-IQ HA**.
5. Click the name of the primary BIG-IQ.
6. On the left, click **Software Version**.
7. Click the **Update** button.
8. From the **Software Image** list, select the image you want to install.
9. From the **Target Volume** list, select the volume you want to install the image on.
10. To prompt BIG-IQ to reboot into the new software installation volume, select the **Reboot into Target Volume** check box.
11. Click the **Apply** button.
12. Click the **Continue** button.
13. Wait while BIG-IQ loads the new software and reboots.

    Depending on your configuration and the number of devices you are managing, this could take up to an hour. During this time, it is important that you not interrupt the installation process by restarting services or the server.

14. If needed, extend the /var partition.

    The default size of the /var file system in a newly installed node is 10 GB. This volume size might be insufficient to store your data. You can see how to extend this file system to a larger size in knowledge article K16103. refer to: K16103: Extending disk space on BIG-IQ Virtual Edition at support.f5.com/csp/article/K16103. Because upgrading a node requires at least two volumes, you must ensure that both volumes can have their /var file system extended to the same size, or upgrades might fail.

15. Log back in to the primary BIG-IQ with your admin user name and password, and complete the setup wizard.

Even though you can log in to the primary BIG-IQ after the software is installed, the system continues some database re-indexing processes in the background. For larger configurations, that can take up to an hour. If you perform any searches on objects before it's done re-indexing, BIG-IQ might not return the expected results. During this time, you can continue with the rest of the upgrade process.

## Upload the BIG-IQ version 5.2 software image

Before you can upload the software image to your BIG-IQ® system, you must have first downloaded it from the F5 Downloads site.

Upload the BIG-IQ version 5.2 software image to your BIG-IQ system to make it available for this upgrade.

1. At the top of the screen, click **System Management**.
2. At the top of the screen, click **Inventory**.
3. On the left, click **SOFTWARE MANAGEMENT** > **Available Images**.
4. Click the **Upload Image** button.
5. Click the **Choose File** button and navigate to the location to which you downloaded the image, and click the **Open** button to upload it to BIG-IQ.
6. Click the **Upload** button.

   The screen refreshes to display the progress of the upload.

When the image is done uploading, it shows in the Available Images list.

## Install version 5.2 on the secondary BIG-IQ system

After you upgrade the primary BIG-IQ® Centralized Management system to version 5.2, you can upgrade a secondary BIG-IQ system for an HA configuration.

You need at least two volumes to install BIG-IQ software. If you are running BIG-IQ Virtual Edition and you don't have two volumes, refer to: *K17406: Using the tmsh utility to create a new software volume for installing a new image or hotfix on the BIG-IQ system* at `https://support.f5.com/csp/article/K17406`.

---

***Important:*** *Be sure you have the Master Key pass phrase you used for the primary BIG-IQ system; you'll need this when you complete the setup wizard after you reboot. You must use the same Master Key pass phrase on both systems for the pair to successfully communicate and synchronize.*

---

Install version 5.2 on a secondary BIG-IQ system so it'll be running the same version as the peer BIG-IQ system you just upgraded.

1. Log on to the system you are going to establish as the secondary BIG-IQ system's command line as **root** and type the following command: `/usr/bin/clear-rest-storage`.

While this step is not required, it clears the database storage on the system so the upgrade goes more quickly. Once upgraded, the primary BIG-IQ will synchronize its database with the secondary BIG-IQ and repopulate the database.

2. Log on to the system you are going to establish as the secondary BIG-IQ system's user interface.
3. If you ran the `clear-rest-storage` command, complete the setup wizard. Otherwise, continue to step 4.
4. At the top of the screen, click **System Management**.
5. At the top of the screen, click **Inventory**.
6. On the left, click **BIG-IQ HA**.
7. Click the secondary BIG-IQ system.
8. On the left, click **Software Version**.
9. Click the **Update** button.
10. From the **Software Image** list, select the image you want to install.
11. To prompt BIG-IQ to reboot into the new software installation volume, select the **Reboot into Target** volume check box.
12. From the **Target Volume** list, select the volume you want to install the image on.
13. Click the **Apply** button.
    A popup screen opens, prompting you to confirm the installation.
14. Click the **Continue** button.
15. Wait while BIG-IQ loads the new software and reboots.

    Depending on your configuration and the number of devices you are managing, this could take up to an hour. During this time, it is important that you not interrupt the installation process by restarting services or the server.
16. Log in to the secondary BIG-IQ system with your admin user name and password.
17. Complete the setup wizard.
18. If needed, extend the /var partition.

    The default size of the /var file system in a newly installed node is 10 GB. This volume size might be insufficient to store your data. You can see how to extend this file system to a larger size in knowledge article K16103. refer to: K16103: Extending disk space on BIG-IQ Virtual Edition at support.f5.com/csp/article/K16103. Because upgrading a node requires at least two volumes, you must ensure that both volumes can have their /var file system extended to the same size, or upgrades might fail.

You can now re-establish the BIG-IQ HA configuration.

## Re-establish the HA configuration after upgrading to BIG-IQ version 5.2

After you upgrade both F5® BIG-IQ® Centralized Management systems in a HA configuration, you can re-associate the secondary system with the primary BIG-IQ system.

1. Log in to primary BIG-IQ system with your administrator user name and password.
2. At the top of the screen, click **System**.
3. On the left, click **BIG-IQ HA**.
4. Click the **Add Secondary** button.
5. In the **IP Address** field, type the discovery address you specified on the BIG-IQ system during setup.

   This is the same IP address the peers in a high availability confirmation use to communicate.
6. In the **User name** and **Password** fields, type the administrative user name and password for the system.

7. In the **Root Password** field, type the root password for the system.
8. Click the **Add** button to add this device to this high availability configuration.

Even though you can log in to the secondary BIG-IQ after the you re-establish the HA configuration, the system continues some database re-indexing processes in the background. For larger configurations, that can take up to an hour. If you perform any searches on objects before it's done re-indexing, BIG-IQ might not return the expected results. During this time, you can use the primary BIG-IQ.

Next, you should verify that both BIG-IQ systems have the same configuration.

## Upgrade the BIG-IP framework

To properly communicate, BIG-IQ® Centralized Management and managed BIG-IP® devices must be running a compatible version of its framework. If the frameworks are incompatible, BIG-IQ displays a yellow triangle next to the device in the BIG-IP Device inventory.

When you upgrade a BIG-IP device running version 11.5.x to another 11.5.x version, or to an 11.6.x version (for example, from version 11.5.3 to 11.5.4, or from version 11.5.3 to version 11.6.1), you must upgrade the REST framework so BIG-IQ can manage the device.

When you upgrade BIG-IQ from version 5.x to 5.2, you must also upgrade the REST framework for all BIG-IP devices (currently in the BIG-IP Device inventory) running a version prior to 12.0.0.

1. At the top of the screen, click **Devices**.
2. Select the check box next to a device, click the **More** button, and select **Upgrade Framework**.
   A popup screen opens.
3. Into the fields, type the required credentials, and click the **Continue** button.
   A `REST Framework upgrade in progress` message displays.

After the framework is updated, you can successfully manage this device.

Repeat these steps for each device.

## Re-discover devices and re-import LTM, ASM, AFM, and DNS services in bulk using a script

After you upgrade to BIG-IQ® Centralized Management version 5.2, you can use a script to re-discover devices and re-import the LTM, ASM, AFT, and DNS services in bulk. To run this script, you must have root access to the BIG-IQ command line.

---

***Warning:*** *Before you run this script, make sure you don't have any pending configuration changes staged for your managed BIG-IP devices. This script prompts BIG-IQ to import the configurations for all your BIG-IP devices. So, if you don't deploy staged configuration changes before you run this script, you will lose them after you run the script. If you need assistance, contact F5 Support.*

---

Use this script to re-discover devices and re-import LTM, ASM, AFT, and DNS services all at once, so you can start managing your devices with the new version of BIG-IQ software.

---

***Note:*** *If you'd rather re-discover devices and re-import their services individually through the user interface, refer to Re-discover devices and re-import LTM, ASM, AFM, and DNS services from the user interface.*

---

1. Log in to the `downloads.f5.com` site, click the **Find a Download** button, and click BIG-IQ **Centralized Management**.

2. Click the **v5.2.0** link.
3. Review the End User Software License agreement and click the **I Accept** button to accept the terms. The Select a Download screen opens.
4. Click the `bulkDiscovery.zip` file name, and unzip it on your local system.
5. Log in to the BIG-IQ system as the root user and upload the script.
6. Enable executable permissions, by typing: `chmod +x ./bulkDiscovery.pl`

   ***Note:*** *To access help for this script, type* `./bulkDiscovery.pl -h`

7. Export the IP addresses for the BIG-IP devices in your network to a CSV file, by typing: `./bulkDiscovery.pl -c masterDeviceList.csv -m -o`
8. Re-discover your BIG-IP devices and re-import their services, by using the associated command:

   ***Note:*** *This command prompts BIG-IQ to import all the configurations from the specified BIG-IP devices. It's important that you've already deployed any configuration changes you have staged for these devices, because they'll be overwritten on BIG-IQ after you run this script. If you'd rather re-discover devices and re-import services individually so you can address any potential configuration conflicts for each device, you can do that from the BIG-IQ system's user interface instead of using this script. For more information, refer to, Re-discover devices and re-import services from the user interface.*

   - For LTM, type `./bulkDiscovery.pl -c myDeviceList.csv -l -m`

     ***Note:*** *You must re-discover devices running the LTM service before re-discovering devices running any other service.*

   - For ASM, type `./bulkDiscovery.pl -c myDeviceList.csv -l -s -m`
   - For AFM, type `./bulkDiscovery.pl -c myDeviceList.csv -l -f -m`
   - For DNS, type `./bulkDiscovery.pl -c myDeviceList.csv -l -d -m`

You can now start managing your BIG-IP devices using BIG-IQ Centralized Management version 5.2.0.

## Re-discover devices and re-import LTM, ASM, AFM, and DNS services from the user interface

After you upgrade F5® BIG-IQ Centralized Management to version 5.2, you must rediscover your managed devices and reimport the services you use so you can start using the new features introduced in this release. This process requires you rediscover each device individually and reimport its services.

***Important:*** *If you'd rather run a Perl script to perform a bulk rediscovery of your devices and reimport of their services, refer to Re-discover devices and re-import LTM, ASM, AFM, and DNS services using a bulk script.*

1. At the top of the screen, click **Devices**.
2. Click the name of the device you want to rediscover and reimport services for.
3. On the left, click **Services**.
4. ***Important:*** *To avoid any unnecessary conflicts between services, re-discover and re-import the LTM service first, before any other services.*

   Click the **Re-discover** button next to a service.
   When BIG-IQ rediscovers the service, a yellow triangle next to the **Re-import** button displays to indicate you need to re-import the service.

5. Click the **Re-Import** button.
6. If there are conflicts, select one of the following options for each object that is different, and then click the **Continue** button:
   - **Use BIG-IQ** to use the configuration settings stored on BIG-IQ.
   - **Use BIG-IP** to override the configuration setting stored on BIG-IQ with the settings from the BIG-IP device.

Perform these steps for the rest of your managed devices.

## Use a script to remove and recreate access groups in bulk for devices running APM services

After you upgrade F5 BIG-IQ Centralized Management to version 5.2, you must remove and recreate the access groups for devices running the APM service.

***Warning:*** *Before you run this script, make sure you don't have any pending configuration changes staged for your managed BIG-IP devices. This script prompts BIG-IQ to import the configurations for all your BIG-IP devices. So, if you don't deploy staged configuration changes before you run this script, you will lose them after you run the script. If you need assistance, contact F5 Support.*

You can use this script to remove and recreate the access groups for devices running the APM service so you can start managing those devices with the new version of BIG-IQ.

***Note:*** *If you'd rather do this from the user interface, refer to, Remove and recreate access groups (with SWG data) from the user interface for devices running APM services or Reimport access groups (without SWG data) from the user interface for devices running APM services.*

1. Log in to the BIG-IQ system as admin.
2. At the top of the screen, select **Configuration**, then expand **ACCESS** and click **Access Groups** .
3. In a separate file (such as a Notepad or Excel file), make a note of:
   - Each access group and the IP addresses of the devices contained within each.
   - The source device, from which you want to copy the configuration to all devices in the access group.

   ***Note:*** *You'll deploy the configuration from this source device to all of the devices in the access group.*
4. Select the check box next to each access group and click the **Remove** button.
5. Log in to the `downloads.f5.com` site, click the **Find a Download** button, and click BIG-IQ **Centralized Management**.
6. Click the **v5.2.0** link.
7. Review the End User Software License agreement and click the **I Accept** button to accept the terms. The Select a Download screen opens.
8. Click the `bulkDiscovery.zip` file name, and unzip it on your local system.
9. Log in to the BIG-IQ system as the root user and upload the script.
10. Enable executable permissions, by typing: `chmod +x ./bulkDiscovery.pl`

    ***Note:*** *To access help for this script, type* `./bulkDiscovery.pl -h`
11. Export the IP addresses for the BIG-IP devices in your network to a CSV file, by typing: `./bulkDiscovery.pl -c masterDeviceList.csv -m -o`

12. For each access group:
    a) Create a device list, by typing `cp masterDeviceList.csv <access_group_name>_devices.csv`
    b) Edit the file as follows:
        - Remove any devices that don't belong to the access groups by comparing it to the list you made in step 3.
        - Place the source BIG-IP device you identified in step 3, at the top of the `<access_group_name>_devices.csv` file.
        - Verify the credentials for each device (the script uses ADMIN/APWD by default).
    c) Save your changes to the file.
    d) Impot devices in the access group by, typing: `./bulkDiscovery.pl -c <access_group_name>_devices.csv -g <access_group_name> -l -p -o -v`
13. Log in to the BIG-IQ system as admin.
14. At the top of the screen, select **Configuration**, then expand **ACCESS** and click **Access Groups** .
15. Review the access groups to verify all the groups properly imported.

You can now start managing your BIG-IP devices using BIG-IQ Centralized Management version 5.2.0.

## Re-import access groups (without SWG data) from the user interface for devices running APM services

After you upgrade F5® BIG-IQ Centralized Management to version 5.2, you must re-import the access groups running the APM service without SWG data.

Use this procedure to access groups for devices running APM services without F5 Secure Web Gateway configuration data so you can start using the new features introduced in this release.

---

***Important:*** *If you'd rather use a script to do this, Use a script to remove and recreate access groups in bulk for devices running APM services. If your APM configuration includes SWG data, refer to Remove and recreate access groups (with SWG data) from the user interface for devices running APM services.*

---

1. At the top of the screen, select **Configuration**, then expand **ACCESS** and click **Access Groups** .
2. Click the name of the access group.
3. From the Device list, select from which to reimport the shared access policy configuration and click the **Reimport** button.

   This device will share the access policy configuration with all other devices in this access group.
4. Select **Shared Access Group and Device Specific configuration** and click the **Reimport** button at the bottom of the screen.
5. If the differences window displays for the LTM service, select **USE_BIGIP** and click the **Resolve** button.
6. If the differences window displays for the APM service, click the **Accept** button.
7. For the remainder of the devices in this access group:
    a) Select the check box next to the device, and click the **Reimport** button.
    b) Select **Device specific configuration** and click the **Reimport** button at the bottom of the screen.
    c) If the differences window displays for the LTM service, select **USE_BIGIP** and click the **Resolve** button.
    d) If the differences window displays for the APM service, click the **Accept** button.
8. Repeat steps 2-7 for the rest of the access groups.

You can now start managing your BIG-IP devices using BIG-IQ Centralized Management version 5.2.0.

## Remove and recreate access groups (with SWG data) from the user interface for devices running APM services

After you upgrade F5® BIG-IQ Centralized Management to version 5.2, you must recreate the access groups running the APM service.

Use this procedure to remove and recreate access groups for devices running APM services with F5 Secure Web Gateway configuration data so you can start using the new features introduced in this release.

***Important:*** *If you'd rather use a script to do this, refer to Use a script to remove and recreate access groups in bulk for devices running APM services. If your APM configuration doesn't include SWG data, refer to Reimport access groups (without SWG data) from the user interface for devices running APM services.*

1. At the top of the screen, select **Configuration**, then expand **ACCESS** and click **Access Groups** .
2. In a separate file (such as a Notepad or Excel file), make a note of:
   - Each access group and the IP addresses of the devices contained within each.
   - The source device, from which you want to copy the configuration to all devices in the access group.

     ***Note:*** *You'll deploy the configuration from this source device to all of the devices in the access group.*
3. Select the check box next to each access group and click the **Remove** button.
4. Click the **Create** button.
5. Type a name for this access group in the **Name** field.
6. From the Device list, select from which to reimport the shared access policy configuration and click the **Reimport** button.

   This device will share the access policy configuration with all other devices in this access group.
7. Click the **Create** button at the bottom of the screen.
8. If the differences window displays for the LTM service, select **USE_BIGIP** and click the **Resolve** button.
9. Click the name of the access group you added.
10. Click the **Add Device** button.
11. From the Device list, select a device to add to this access group.
12. Click the **Add** button at the bottom of the screen.
13. If the differences window displays for the LTM service, select **USE_BIGIP** and click the **Resolve** button.
14. If the differences window displays for the APM service, click the **Accept** button.
15. Repeat these steps 10-14 for each device in each access group before creating the next access group.

You can now start managing your BIG-IP devices using BIG-IQ Centralized Management version 5.2.0.

# Prepare the Data Collection Device Cluster for Data Restoration

## Define external storage snapshots location

Before you can configure the external snapshot storage location, you need the following information for the machine you will use to store your data collection device (DCD) snapshots:

- Storage-machine-IP-address
- Storage-file-path
- User name, password, and (optionally) the domain for the user account configured on the external storage device
- Read/Write permissions for the storage file path

You need snapshots to perform software upgrades and to restore your old data.

When you create DCD snapshots, they need to be stored on a machine other than the DCD. You define the location for the snapshot using the BIG-IQ® Centralized Management device.

1. At the top of the screen, click **System**.
2. On the left, expand **BIG-IQ DATA COLLECTION** and then select **BIG-IQ Data Collection Devices**.
   The BIG-IQ Data Collection Devices screen opens to display the currently defined data collection device cluster.
3. Click the **Settings** button.
   The Settings screen opens to display the current state of the DCD cluster defined for this BIG-IQ device.
4. For **External Storage**, click **Configure**.
   The External Storage popup screen opens.
5. In the **User name** and **Password** fields, type the user name and password for the user account configured on the external storage device.
6. For the **Domain**, type in the domain name for the user account configured on the external storage device.
7. For the **Storage Path**, type the path to the external storage location.

   You can specify the device using the IP address or the host name. Additionally, you need to specify the path to the folder on the external storage device. For example:

   ```
   //<storage machine ip-address>/<storage-file-path>
   ```

   ***Note:*** *Remember, the folder you specify must have full read, write, and execute permissions.*
8. To test the settings just specified, click **Test**.
   A message displays to tell you whether the test completes successfully. If it does not, correct the settings and permissions until it completes successfully.
9. When the external storage is specified successfully, click **Save**.

The storage location should now be accessible to the all of the devices in the DCD cluster.

## Restart data collection device cluster

If too much time elapses between the time you upgrade the data collection devices in your cluster, the cluster communication between data collection devices can fail. If the communication fails, some of the

devices can fail to re-join the cluster. If one of the devices does not re-join the cluster, the cluster will not operate. To prevent this scenario, you need to restart the cluster before proceeding.

***Note:*** *You must perform this task on each device in the cluster (that is, each data collection device, the BIG-IQ® Centralized Management device, and the BIG-IQ HA peer).*

1. Use SSH to log in to a device in the cluster.
   You must log in as `root` to perform this procedure.
2. Run the following command to restart the cluster on this device:
   `bigstart restart elasticsearch`
3. Run the following command to confirm that the cluster restarted on this device:
   `bigstart status elasticsearch`
4. Repeat the previous three steps for each device in the cluster.

Once you have restarted the cluster for each device, you can proceed to the next task.

## Check data collection device health

You can use the Logging Configuration screen to review the overall health and status of the data collection devices you've configured. You can use the data displayed on this screen both before and after an upgrade to verify that your data collection device cluster configuration is as you expect it to be.

1. At the top of the screen, click **System**.
2. On the left, expand **BIG-IQ DATA COLLECTION** and then select **BIG-IQ Data Collection Devices**.
   The BIG-IQ Data Collection Devices screen opens to display the currently defined data collection device cluster.
3. Click the **Settings** button.
   The Settings screen opens to display the current state of the DCD cluster defined for this BIG-IQ device.
4. Check the cluster health status. If there are any cluster health issues, resolve those issues and then repeat the process until the cluster is operating normally.

## Restore data collection device snapshots

You can use the BIG-IQ® user interface to restore data collection device (DCD) snapshots.

Please note:

- The restore operation requires a down time during which no BIG-IQ or DCD work is performed.
- During the restore operation, no data sent to the DCD is retained.
- The restore operation restores only the data from the time before the chosen snapshot was created. Data from the time that the chosen snapshot was created to the current time is not restored.
- Before initiating a snapshot restore, make sure that sufficient disk space is allocated to the /var folder on the device to which you are restoring the snapshot.

1. At the top of the screen, click **System**.
2. On the left, expand **BIG-IQ DATA COLLECTION** and then select **BIG-IQ Data Collection Devices**.
   The BIG-IQ Data Collection Devices screen opens to display the currently defined data collection device cluster.
3. Click the **Settings** button.

The Settings screen opens to display the current state of the DCD cluster defined for this BIG-IQ device.

4. You have two options for choosing a snapshot and starting the restore, using the settings in the External Storage & Snapshot area near the bottom of the screen.

| Option | Description |
|---|---|
| **To restore from the most recent snapshot:** | Next to **Last Snapshot/Time**, click **Restore Latest**. |
| **To select the snapshot that you want to restore:** | 1. Click the **View History** button.<br>2. Choose the snapshot you wish to restore, and click **Restore**. |

## Activate data collection devices services

To upgrade your data collection devices, you deactivated all data collection device services. Once the upgraded software is installed, you must activate the services before you can resume normal operation.

***Note:*** *Perform this action on the BIG-IQ® Centralized Management device; not the data collection device (DCD).*

1. At the top of the screen, click **System**.
2. On the left, expand **BIG-IQ DATA COLLECTION** and then select **BIG-IQ Data Collection Devices**.
   The BIG-IQ Data Collection Devices screen opens to display the currently defined data collection device cluster.
3. Click a DCD name.
   The Properties screen for the selected device opens.
4. On the left, click **Services**.
5. For each service that you use, click **Activate**.
6. Click **Close**.
7. Repeat the steps for each DCD in the cluster.

This restarts the services on your DCDs.

## Recheck data collection device health

You can use the Settings screen to review the overall health and status of the data collection devices you've configured. You can use the data displayed on this screen both before and after an upgrade to verify that your data collection device cluster configuration is as you expect.

1. At the top of the screen, click **System**.
2. On the left, expand **BIG-IQ DATA COLLECTION** and then select **BIG-IQ Data Collection Devices**.
   The BIG-IQ Data Collection Devices screen opens to display the currently defined data collection device cluster.
3. Click the **Settings** button.
   The Settings screen opens to display the current state of the DCD cluster defined for this BIG-IQ device.
4. Analyze the data collection device cluster details listed in the Summary area, and make sure that the values after upgrade match the values from the health check you did before the upgrade.

- Devices in Cluster
- Total Document Count
- Total Document Size

This information provides a fairly detailed overview that describes the data collection device cluster you have created to store alerts and event log data.

5. Check the cluster health status. If there are any cluster health issues, resolve those issues and then repeat the process until the cluster health is as you expect it to be.

## Recover from an unsuccessful upgrade

To recover from an unsuccessful upgrade, you need to know the volume names for the volumes into which the pre- and post- upgrade versions were installed.

If you complete the upgrade process and the cluster configuration is not the same as before the upgrade, the upgrade was unsuccessful. You need a way to repeat the process.

1. Use SSH to log in to the BIG-IQ Centralized Management device.

   You must log in as `root` to perform this process.

2. Reboot the BIG-IQ device into the volume that you used for the previous version BIG-IQ.
   From the command prompt type: `tmsh reboot volume <pre-upgrade volume name>`
   The device reboots. The device goes offline. When it comes back online, you can proceed.
3. When the device reboot is complete, restart the upgrade process from the beginning. Take particular care to follow the work flow precisely. If you did not use the command line method the first time, we highly recommend using it to increase the likelihood of success.

# Legal Notices

## Legal notices

### Publication Date

This document was published on May 5, 2017.

### Publication Number

MAN-0642-02

### Copyright



### Trademarks

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

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

### Patents

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

### Export Regulation Notice

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

### RF Interference Warning

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

### FCC Compliance

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

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

### Canadian Regulatory Compliance

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

### Standards Compliance

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

# Index