DEPLOYMENT GUIDE

DEPLOYING THE BIG-IP LTM SYSTEM WITH ADOBE ACROBAT CONNECT PROFESSIONAL

Deploying the BIG-IP LTM system with Adobe Acrobat Connect Professional

Welcome to the F5 - Adobe® Acrobat Connect™ Professional Deployment Guide. This guide provides step-by-step procedures for configuring the BIG-IP LTM system with Adobe Connect Professional (formerly Breeze) server pools.

Adobe Acrobat Connect Professional provides scalable Web conferencing with extensive meeting management capabilities that enable business professionals to communicate and collaborate instantly with extended teams and large audiences through easy-to-use and easy-to-access online personal meeting rooms.

For more information on Adobe Connect Professional, see **http://www.adobe.com/products/acrobatconnectpro/**

Prerequisites and configuration notes

All of the procedures in this Deployment Guide are performed on the BIG-IP system. The following are prerequisites for this solution:

- Adobe Connect Professional should be running Adobe Connect Enterprise Server 6 SP3 with the SP3 Security Patch, or a later version. See the ***Adobe Installation and Configuration Guide*** for Adobe configuration information.
- For this Deployment Guide, the BIG-IP LTM system must be running version 9.0 or later. We recommend running version 9.4.2 or later.
- We assume that the BIG-IP LTM device is already installed in the network, and objects like Self IPs and VLANs have already been created. For more information on configuring these objects, see the BIG-IP LTM documentation, available on Ask F5 (**https://support.f5.com/**).
- In this guide, we assume that the BIG-IP LTM system will be offloading SSL. SSL acceleration is performed on the BIG-IP LTM rather than on the Connect servers. For SSL offload, you must already have obtained an SSL Certificate (but not necessarily installed it on the BIG-IP LTM system). For information on configuring Adobe Connect Enterprise for SSL, see **help.adobe.com/en_US/Connect/6.0/InstallationConfiguration/ssl.pdf**

Configuration example

In this deployment, the BIG-IP LTM system is first terminating SSL and directing traffic to one of the Adobe Connect servers. The Connect server assigns the client to the appropriate session on the Acrobat Connect Meeting

(Flash Media) server. When the client returns to the BIG-IP LTM after the session has been defined, the LTM offloads the SSL, and sends the traffic on to the server that hosts the appropriate session.

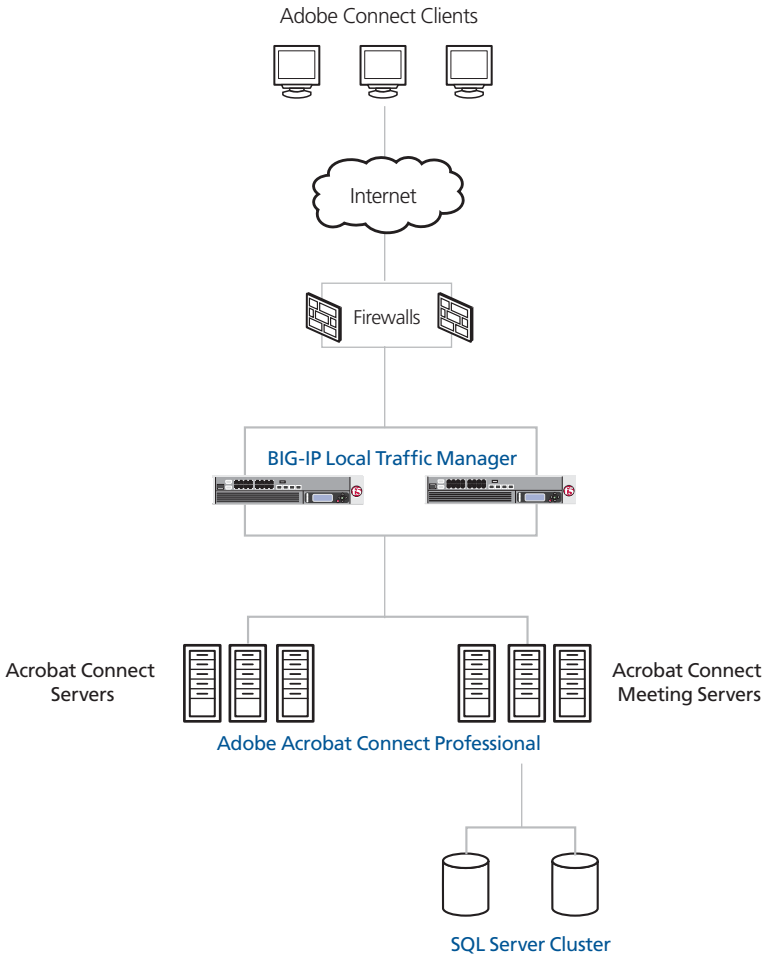

Figure 1 *Logical configuration example*

Configuring the BIG-IP LTM system for Connect Professional devices

To configure the BIG-IP LTM system to direct traffic to the Connect Professional servers, you need to complete the following tasks:

- *Creating the health monitors*
- *Creating the pools*
- *Creating profiles*
- *Creating the virtual servers*

Creating the health monitors

The first step is to set up health monitors for the Connect Professional devices. These procedures are optional, but very strongly recommended. In our example, we create an advanced HTTP health monitor, a TCP monitor and a simple ICMP node health check.

Creating the HTTP health monitor

The first health check we configure is an HTTP monitor that uses Send and Receive strings to ensure that the target device is not only up, but serving the proper content. The Send and Receive strings are optional.

To create the HTTP health monitor

1. On the Main tab, expand **Local Traffic**, and then click **Monitors**.
2. Click the **Create** button. The New Monitor screen opens.
3. In the **Name** box, type a name for the Monitor.
   In our example, we type **connectpro-http**.
4. From the **Type** list, select **http**.
5. In the Configuration section, in the **Interval** and **Timeout** boxes, type an Interval and Timeout. We recommend at least a 1:3 +1 ratio between the interval and the timeout (for example, the default setting has an interval of **5** and an timeout of **16**). In our example, we use a **Interval** of **30** and a **Timeout** of **91** (see Figure 2).
6. In the **Send String** box, type an appropriate Send String. In our example, we point the monitor at the testbuilder diagnostic page, as the testbuilder is probing the Connect Professional database to make sure there is a healthy connection. In our example, we type

   ```
   GET /servlet/testbuilder HTTP/1.0\r\nHost:
   adobe.com\nConnection:close\r\n\r\n
   ```

   The host name in this example (**adobe.com**) should match the name of the site being checked.
7. In the **Receive String** box, type an appropriate Receive String. In our example, we expect the testbuilder to return **status-ok**, so we type **status-ok** in the box.
8. Click the **Finished** button (see Figure 2).
   The new monitor is added to the Monitor list.

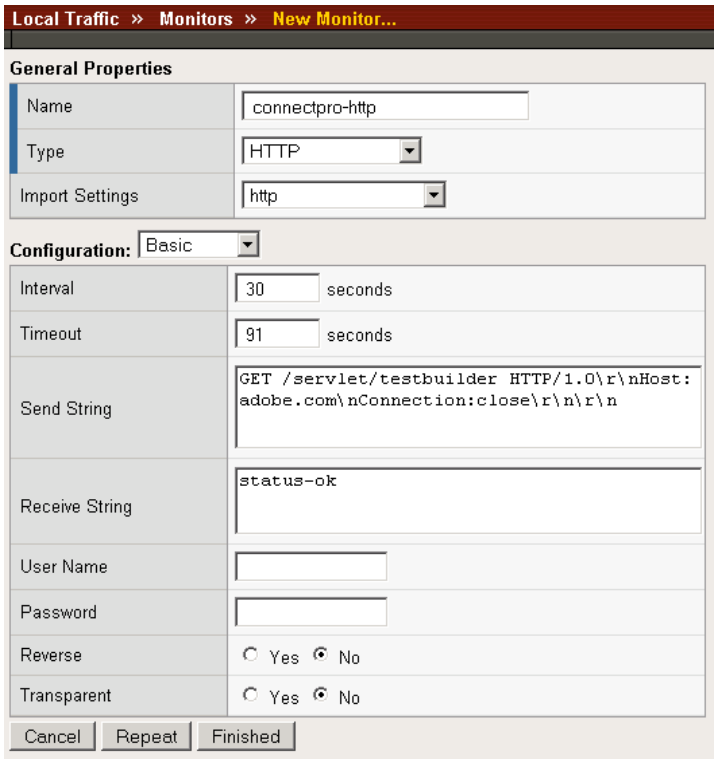

Figure 2 *Creating the HTTP Monitor*

Creating the TCP monitor

The next monitor we create is a TCP health check to monitor, which will be used in the single server pools in the following section.

To create the TCP health monitor

1. On the Main tab, expand **Local Traffic**, and then click **Monitors**.
2. Click the **Create** button. The New Monitor screen opens.
3. In the **Name** box, type a name for the Monitor.
   In our example, we type **connectpro-tcp**.
4. From the **Type** list, select **tcp**.
5. In the Configuration section, in the **Interval** and **Timeout** boxes, type an Interval and Timeout. We recommend at least a 1:3 +1 ratio between the interval and the timeout (for example, the default setting has an interval of **5** and an timeout of **16**). In our example, we use a **Interval** of **30** and a **Timeout** of **91**.
6. Configure the rest of the settings as applicable for your deployment.
7. Click the **Finished** button.

Creating the ICMP monitor

The final monitor we create is a ICMP health check that simply pings the node address, and marks the node down if it does not respond. In our example, we create a Default Node Monitor, which assigns the monitor to all of the nodes that the BIG-IP LTM system is aware of. If you wish to create a monitor specific to the Connect Professional nodes, follow the preceding procedure, but in step 4, select **ICMP**.

To create a Default Node Monitor

1. On the Main tab, expand **Local Traffic**, and then click **Nodes**.
   The Nodes List opens.
2. On the Menu bar, click **Default Monitor**.
3. From the **Available** list, select ICMP, and then click the Add (**<<**) button.
4. Click the **Update** button.

Creating the pools

The next step is to define load balancing pools for the Connect Professional servers. In this section, we create a pool for each of the Connect Professional devices in the configuration, and then one pool that contains all of the Connect Professional devices. We configure a pool for each server so that once the initial connection is load balanced to a Connect Professional device, the return traffic is directed to the appropriate device.

Creating the Connect Professional pool

The first pool we create contains all of the Adobe Connect Professional devices in this configuration, and uses the advanced health check monitor you created in *Creating the HTTP health monitor*, on page 3.

1. On the Main tab, expand **Local Traffic**, and then click **Pools**.
   The Pool screen opens.
2. In the upper right portion of the screen, click the **Create** button.
   The New Pool screen opens.
3. In the **Name** box, type a name for your pool.
   In our example, we use **connectpro-pool**.
4. In the **Health Monitors** section, select the name of the monitor you created in the *Creating the HTTP health monitor* section, and click the Add (**<<**) button. In our example, we select **connectpro-http**.
5. From the **Load Balancing Method** list, choose your preferred load balancing method (different load balancing methods may yield optimal results for a particular network).
   In our example, we select **Round Robin**.
6. In this pool, we leave the Priority Group Activation **Disabled**.

7. In the New Members section, make sure the **New Address** option button is selected.
8. In the **Address** box, add the first Connect Professional device to the pool. In our example, we type **10.132.81.110**.
9. In the **Service Port** box, type **8443**, or select HTTP from the list.
10. Click the **Add** button to add the member to the list.
11. Repeat steps 8-10 for each Connect Professional device.
12. Click the **Finished** button.

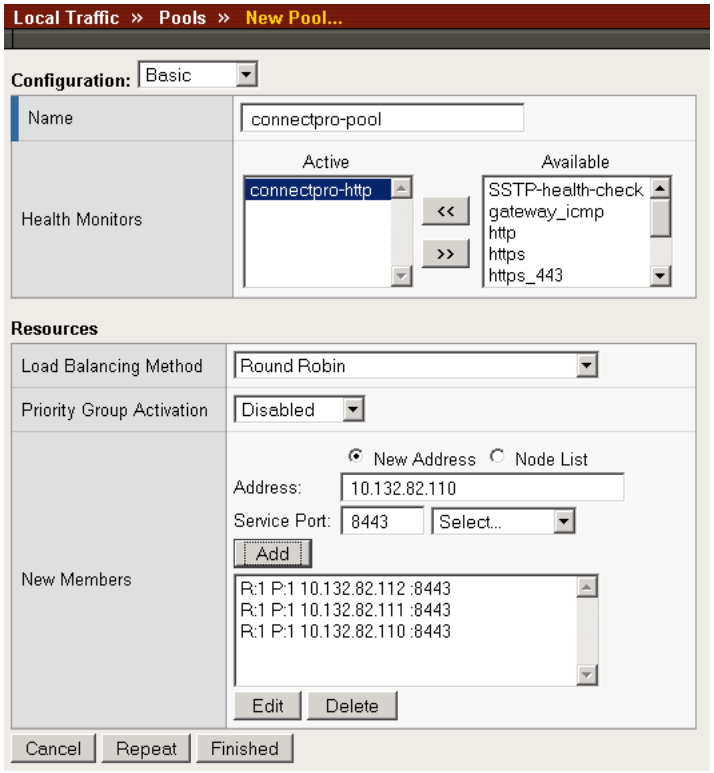

Figure 3 *Creating the pool for the Connect Professional servers*

Creating the single server pools

In this section, we create a separate BIG-IP LTM pool for each Connect Professional device in this deployment. Repeat this entire procedure for each of your Connect Professional devices.

To create the Connect Professional single server pool

1. On the Main tab, expand **Local Traffic**, and then click **Pools**. The Pool screen opens.
2. In the upper right portion of the screen, click the **Create** button. The New Pool screen opens.

3. In the **Name** box, type a name for your pool.
   In our example, we use **connectpro-meetingserver1**.
4. In the **Health Monitors** section, select the name of the monitor you created in the *Creating the TCP monitor* section, and click the Add (**<<**) button. In our example, we select **connectpro-tcp**.
5. Leave the **Load Balancing Method** list at the default setting (as there is only one device in the pool, the load balancing method is not important.
6. In this pool, we leave the Priority Group Activation **Disabled**.
7. In the New Members section, make sure the **New Address** option button is selected.
8. In the **Address** box, add one Connect Professional device to the pool. In our example, we type **10.132.81.110**.
9. In the **Service Port** box, type **1935**, the default port for Adobe RTMP traffic.
10. Click the **Add** button to add the member to the list.
11. Click the **Finished** button.
12. Repeat this entire procedure to create a new pool for each of the Adobe Connect Professional devices in your configuration.

Using SSL certificates and keys

Before you can enable the BIG-IP LTM system to act as an SSL proxy, you must install a SSL certificate on the virtual server that you wish to use for Adobe Connect Professional connections on the BIG-IP LTM device. For this Deployment Guide, we assume that you already have obtained an SSL certificate, but it is not yet installed on the BIG-IP LTM system. For information on generating certificates, or using the BIG-IP LTM to generate a request for a new certificate and key from a certificate authority, see the **Managing SSL Traffic** chapter in the ***Configuration Guide for Local Traffic Management***.

Importing keys and certificates

Once you have obtained a certificate, you can import this certificate into the BIG-IP LTM system using the Configuration utility. By importing a certificate or archive into the Configuration utility, you ease the task of managing that certificate or archive. You can use the Import SSL Certificates and Keys screen only when the certificate you are importing is in Privacy Enhanced Mail (PEM) format.

To import a key or certificate

1. On the Main tab, expand **Local Traffic**.
2. Click **SSL Certificates**. The list of existing certificates displays.

3. In the upper right corner of the screen, click **Import**.
4. From the **Import Type** list, select the type of import (Certificate or Key).
5. In the **Certificate** (or **Key**) **Name** box, type a unique name for the certificate or key.
6. In the **Certificate** (or **Key**) **Source** box, choose to either upload the file or paste the text.
7. Click **Import**.

If you imported the certificate, repeat this procedure for the key.

Creating profiles

BIG-IP version 9.0 and later use profiles. A ***profile*** is an object that contains user-configurable settings for controlling the behavior of a particular type of network traffic, such as HTTP connections. Using profiles enhances your control over managing network traffic, and makes traffic-management tasks easier and more efficient.

Although it is possible to use the default profiles, we strongly recommend you create new profiles based on the default parent profiles, even if you do not change any of the settings initially. Creating new profiles allows you to easily modify the profile settings specific to this deployment, and ensures you do not accidentally overwrite the default profile.

For this configuration, we create four new profiles: an HTTP profile, a TCP profile, a Client SSL profile and a OneConnect profile. We do not use a persistence profile with Adobe Connect Professional.

Creating an HTTP profile

The first new profile we create is an HTTP profile. The HTTP profile contains numerous configuration options for how the BIG-IP LTM system handles HTTP traffic.

To create a new HTTP profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**. The HTTP Profiles screen opens.
2. In the upper right portion of the screen, click the **Create** button. The New HTTP Profile screen opens.
3. In the **Name** box, type a name for this profile. In our example, we type **connectpro-http**.
4. From the **Parent Profile** list, select **http**.
5. Modify any of the other settings as applicable for your network. In our example, we leave the settings at their default levels.
6. Click the **Finished** button.

Creating the TCP profile

The next profile we create is the TCP profile.

To create a new TCP profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**. The HTTP Profiles screen opens.
2. On the Menu bar, from the **Protocol** menu, click **tcp**.
3. In the upper right portion of the screen, click the **Create** button. The New TCP Profile screen opens.
4. In the **Name** box, type a name for this profile. In our example, we type **connectpro-tcp**.
5. From the **Parent Profile** list, select **tcp**.
6. Modify any of the settings as applicable for your network. In our example, we leave the settings at their default levels.
7. Click the **Finished** button.

Creating a Client SSL profile

The profile in this configuration is to create a Client SSL profile. This profile contains the SSL certificate and Key information for decrypting the SSL traffic on behalf of the servers.

To create a new Client SSL profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**.
2. On the Menu bar, from the SSL menu, select **Client**. The Client SSL Profiles screen opens.
3. In the upper right portion of the screen, click the **Create** button. The New Client SSL Profile screen opens.
4. In the **Name** box, type a name for this profile. In our example, we type **connectpro-clientssl**.
5. In the Configuration section, check the **Certificate** and **Key Custom** boxes.
6. From the **Certificate** list, select the name of the Certificate you imported in the *Importing keys and certificates* section.
7. From the **Key** list, select the key you imported in the *Importing keys and certificates* section.
8. Click the **Finished** button.

Creating a OneConnect profile

The final profile we create is a OneConnect profile. With OneConnect enabled, client requests can utilize existing, server-side connections, thus reducing the number of server-side connections that a server must negotiate to service those requests. This can provide significant performance improvements for Connect Professional implementations. For more information on OneConnect, see the BIG-IP LTM documentation.

In our example, we leave all the options at their default settings. You can configure these options as appropriate for your network.

To create a new OneConnect profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**. The HTTP Profiles screen opens.
2. On the Menu bar, from the **Other** menu, click **OneConnect**. The Persistence Profiles screen opens.
3. In the upper right portion of the screen, click the **Create** button.
4. In the **Name** box, type a name for this profile. In our example, we type **connectpro-oneconnect**.
5. From the **Parent Profile** list, ensure that **oneconnect** is selected.
6. Modify any of the other settings as applicable for your network. In our example, we leave the settings at their default levels.
7. Click the **Finished** button.

Creating the virtual servers

The next task is to create virtual servers on the BIG-IP LTM system. In this section, we create a virtual server for each of the single server pools, as well as one for the pool that contains all of the Connect Professional devices.

To create a virtual server

1. On the Main tab, expand **Local Traffic**, and then click **Virtual Servers**. The Virtual Servers screen opens.
2. In the upper right portion of the screen, click the **Create** button. The New Virtual Server screen opens.
3. In the **Name** box, type a name for this virtual server. In our example, we type **connectpro-virtual**.
4. In the **Destination** section, select the **Host** option button.
5. In the **Address** box, type the IP address of this virtual server. In our example, we use **192.168.10.120.**
6. In the **Service Port** box, type **443**, or select **HTTPS** from the list (see Figure 4).

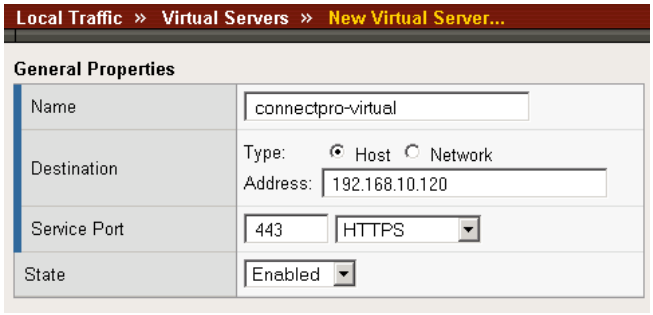

Figure 4 *Creating the Connect Professional virtual server*

7. From the Configuration list, select **Advanced**.
8. From the **Protocol Profile (Client)** list select the name of the profile you created in the *Creating the TCP profile* section. In our example, we select **connectpro-tcp**.
9. From the **Protocol Profile (Server)** list, select the name of the profile you created in the *Creating the TCP profile* section. In our example, we select **connectpro-tcp**.
10. From the **OneConnect Profile** list, select the name of the profile you created in *Creating a OneConnect profile*. In our example, we select **connectpro-oneconnect**.
11. From the **HTTP Profile** list, select the name of the profile you created in the *Creating an HTTP profile* section. In our example, we select **connectpro-http**.
12. From the **Client SSL Profile (Client)** list, select the name of the SSL profile you created in the *Creating a Client SSL profile* section. In our example, we select **connectpro-clientssl**.

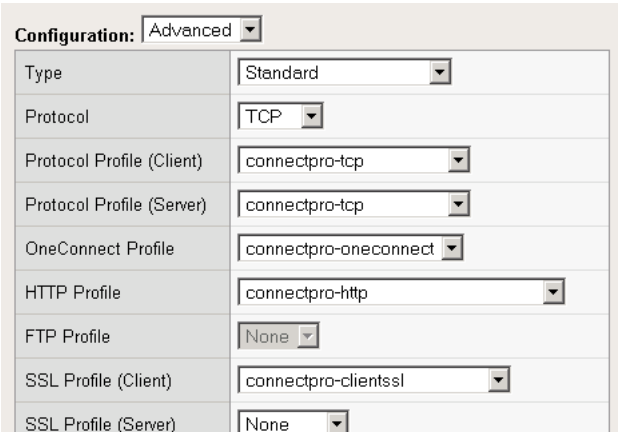

Figure 5 *Selecting the profiles for the virtual server*

13. From the **Default Pool** list, select the pool you created in the *Creating the Connect Professional pool* section. In our example, we select **connectpro-pool**.

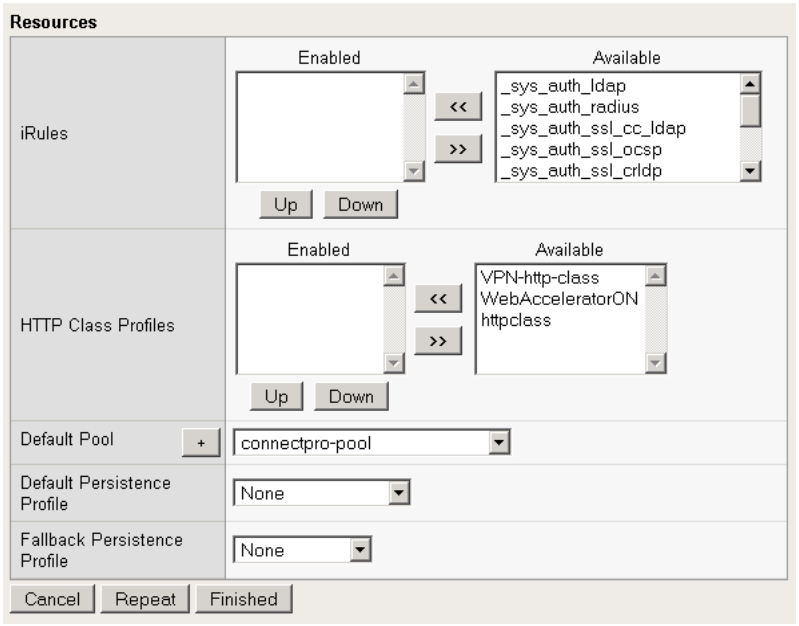

Figure 6 *Adding the Pool and Persistence profile to the virtual server*

14. Click the **Finished** button.
15. Repeat this entire procedure for each of the single server pools, giving each a unique name, and adding the appropriate pool in step 15.

Synchronizing the BIG-IP configuration if using a redundant system

If you are using a redundant BIG-IP configuration, the final step is to synchronize the configuration to the peer BIG-IP device.

To synchronize the configuration using the Configuration utility

1. On the Main tab, expand **System**.
2. Click **High Availability**.
   The Redundancy screen opens.
3. On the Menu bar, click **ConfigSync**.
4. Click the **Self --> Peer** button.
   The configuration synchronizes with its peer.