



Integrating CoroSoft Datacenter Automation Suite with F5 Networks BIG-IP

- Introducing the CoroSoft BIG-IP Solution
- Configuring the CoroSoft BIG-IP Solution
- Optimizing the BIG-IP configuration

Introducing the CoroSoft BIG-IP Solution

Using F5 Networks iControl™ open SDK/API, CoroSoft™ has created a simple, yet powerful way to integrate the BIG-IP® system into a CoroSoft Datacenter Automation Suite deployment, for a unique solution providing unparalleled scalability, security, and high availability.

This solution is suitable for traditional server deployments, but is ideal for blade server systems. When servers reach user-defined thresholds, the CoroSoft Datacenter Automation Suite has ability to quickly allocate blades (or traditional servers) or signal another application, like CoroSoft's PowerCockpit® or the Altiris® Deployment Server, to build or image a blade with an OS and applications and then add it to a network. This combined solution delivers the dense server processing power required by mission critical applications without over provisioning.

Through iControl, when the CoroSoft system determines that more resources are needed based on a Administrator defined policy, it can dynamically instruct BIG-IP to add the new resource to an existing pool of load balanced servers, and remove those servers when they are no longer required.

For more information about iControl, please refer to the F5 Networks Web site at <http://devcentral.f5.com/>.

Prerequisites and configuration notes

In order to use the BIG-IP CoroSoft Solution, the BIG-IP system must be running version 4.1.1 or later.

Before you start to deploy the CoroSoft BIG-IP Solution, you should have already installed all of the components of the CoroSoft Automation Suite. For specific prerequisites and requirements for the CoroSoft Automation Suite, refer to the CoroSoft documentation.

Configuration example

As previously mentioned, the CoroSoft BIG-IP Solution can be run on either a blade server system, or a traditional server system. Figure 1.1 shows the CoroSoft BIG-IP solution in a blade server system and Figure 1.2 shows the solution in a traditional server deployment.

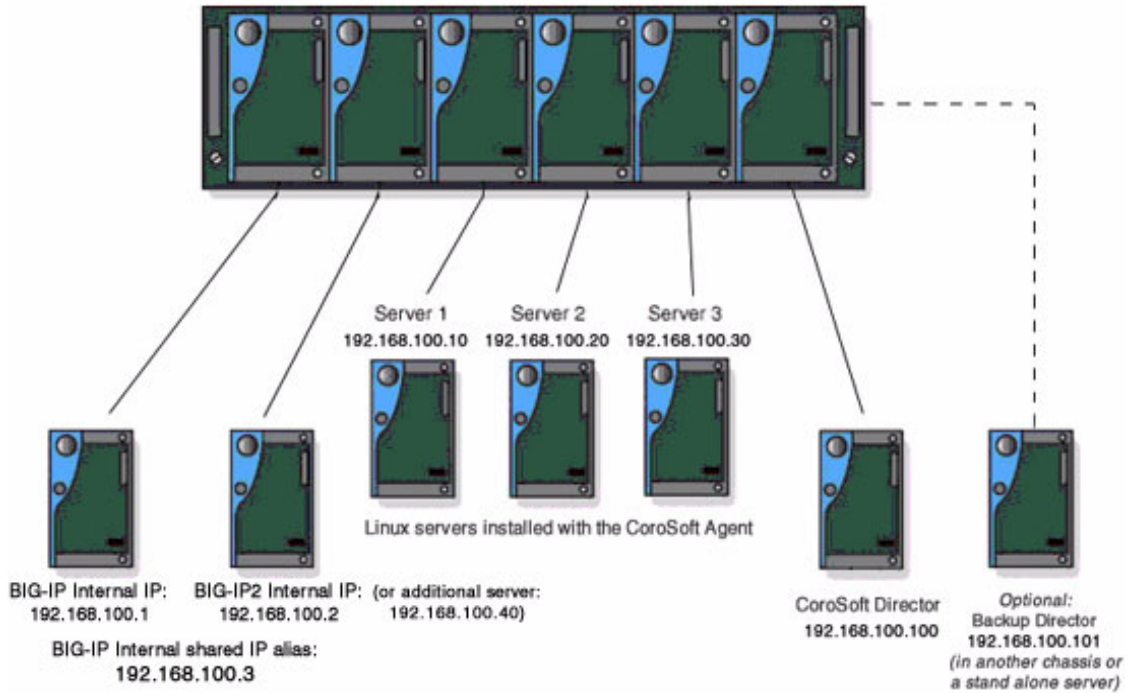


Figure 1.1 CoroSoft BIG-IP deployment on a blade server system

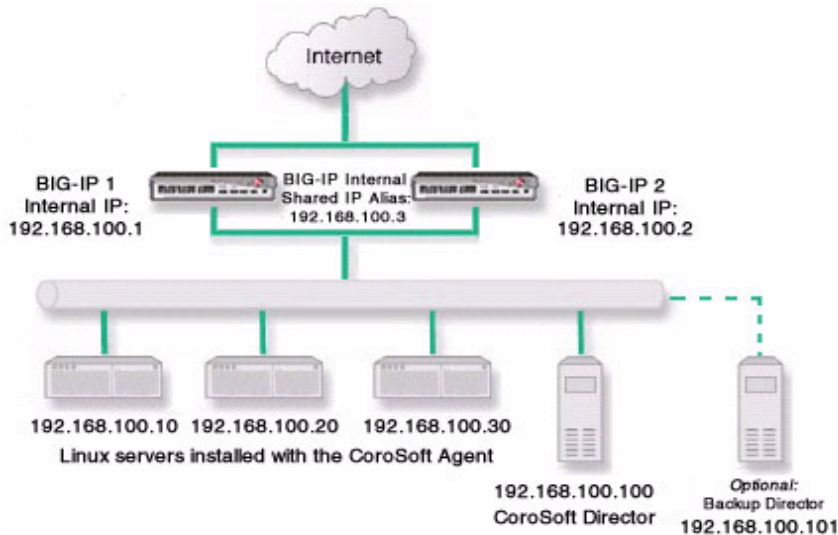


Figure 1.2 Example of a CoroSoft BIG-IP deployment in a traditional network configuration.

◆ **Note**

For the rest of this document, we use the IP addresses shown in the figures above in our examples.

Configuring the CoroSoft BIG-IP Solution

The way you configure the CoroSoft BIG-IP Solution depends on whether you have a new or existing implementation of CoroSoft. If you are adding the BIG-IP system to an existing CoroSoft deployment, or you are deploying CoroSoft for the first time and want to configure the BIG-IP system as the load balancing solution.

- *Deploying CoroSoft for the first time*
- *Adding the BIG-IP to an existing CoroSoft deployment*

Deploying CoroSoft for the first time

If you are initially configuring your CoroSoft Datacenter Automation Suite, use the following procedures:

- *Installing CoroSoft*
- *Configuring the CoroSoft software for the BIG-IP*

Installing CoroSoft

For detailed instructions on how to install the CoroSoft software, refer to the CoroSoft Installation Guide.

Configuring the CoroSoft software for the BIG-IP

After you have installed the CoroSoft software, log in as the **root** user on the CoroSoft Director™ and type the following command to complete the configuration:

```
/usr/sbin/configureDirector
```

This launches a script-based set of questions that gather the information for and set the configuration of the Director and the BIG-IP device.

Just before the `configureDirector` script finishes, it automatically starts another script, **configureLBControl**, which allows you add a BIG-IP to the configuration.

To add a BIG-IP to a new CoroSoft installation

1. Install the software according to the CoroSoft documentation, and run the **configureDirector** script as described above.

- When you see the following screen, type **a**, and press Enter:

```
Corosoft Load Balancer Control Configuration

Currently configured Load Balancers:
-----
                NONE
-----
(a)dd, (F)inished?
```

- When prompted, enter the IP address of the BIG-IP product.

Important Note:

If you have a redundant BIG-IP system (two BIG-IP devices in a active-standby or active-active configuration), enter the **internal shared IP alias** for the IP address of the BIG-IP system. In our example, we use **192.168.100.3**, the internal shared IP alias for our redundant system.

- When prompted for the type of load balancer, type **b** for BIG-IP, and press Enter.

The following message displays:

```
The BIG-IP's SOAP interface will be used, which uses
https commands.
```

- You are then prompted to enter the port the BIG-IP system uses for HTTPS traffic. Press Enter to choose the default port of **443**, or if you modified the BIG-IP configuration to use a port other than **443** for HTTPS, type that port, and press Enter.
- Next, you are prompted for a valid web administration user ID. This user ID is any user name used to access the BIG-IP web-based Configuration utility (GUI) with Full Web Read/Write access. Type the user ID, and press Enter. In our example, we use **admin**.
- Enter the password for the user ID entered above, and press Enter. You are prompted to re-enter the password to verify.
- A summary screen displays with all of the entries, and you are prompted to confirm their accuracy. See the following example:

```
Enter IP address for new Load Balancer to control: 192.168.100.3

Type of load balancer (I)PVS or (B)igIP [IPVS]? B

The BigIP's SOAP interface will be used, which uses https commands.
Enter BigIP's https port [443]: 443
Enter a valid web Administration UserID: admin
Enter password for <userID>:
Re-enter password to verify:

Type: BigIP
IP Address: 192.168.100.254
Port: 443
UserID: admin
Password: *****

Are these correct (y/n)? [n]: y
```

-
9. CoroSoft Director attempts to connect to the BIG-IP system. If the Director cannot connect to the BIG-IP, check the IP address of the BIG-IP and your network connections, and begin this procedure again.

Adding the BIG-IP to an existing CoroSoft deployment

If you are already using CoroSoft, and want to modify the configuration to add a BIG-IP system, use the following procedure.

To add a BIG-IP to an existing CoroSoft deployment

1. Log onto to the command line of the CoroSoft Director as the **root** user.
2. Type the following command to start the configuration script:

```
/usr/sbin/configureLBControl
```

The following screen displays:

```
Corosoft Load Balancer Control Configuration
Currently configured Load Balancers:
-----
                NONE
-----
(a)dd, (F)inished?
```

3. Type **a**, and press Enter.
4. When prompted, enter the IP address of the BIG-IP product.

Important Note:

*If you have a redundant BIG-IP system (two BIG-IP devices in a active-standby or active-active configuration), enter the **internal shared IP alias** for the IP address of the BIG-IP system. In our example, we use **192.168.100.3**, the internal shared IP alias for our redundant system.*

5. When prompted for the type of load balancer, type **b** for BIG-IP, and press Enter.
The following message displays:
The BIG-IP's SOAP interface will be used, which uses https commands.
6. You are then prompted to enter the port the BIG-IP system uses for HTTPS traffic. Press Enter to choose the default port of **443**, or if you modified the BIG-IP configuration to use a port other than **443** for HTTPS, type that port, and press Enter.
7. Next, you are prompted for a valid web administration user ID. This user ID is any user name used to access the BIG-IP web-based Configuration utility (GUI) with Full Web Read/Write access. Type the user ID, and press Enter.
In our example, we use **admin**.

8. Enter the password for the user ID entered above, and press Enter. You are prompted to re-enter the password to verify.
9. A summary screen displays with all of the entries, and you are prompted to confirm their accuracy. See the following example:

```
Enter IP address for new Load Balancer to control: 192.168.100.3

Type of load balancer (I)PVS or (B)igIP [IPVS]? B

The BigIP's SOAP interface will be used, which uses https commands.
Enter BigIP's https port [443]: 443
Enter a valid web Administration UserID: admin
Enter password for <userID>:
Re-enter password to verify:

Type: BigIP
IP Address: 192.168.100.254
Port: 443
UserID: admin
Password: *****

Are these correct (y/n)? [n]: y
```

10. CoroSof Director attempts to connect to the BIG-IP system. If the Director cannot connect to the BIG-IP, check the IP address of the BIG-IP and your network connections, and begin this procedure again.

Configuring CoroSof Services and Policies

CoroSof Automation Suite *Policies* are the rules that let IT administrators automatically bring additional servers online, as well as storage, network and database connections to maintain service levels under heavy usage. There is only one policy per service, but a policy can include as many or as few rules as you need. Services and policies are configured using the CoroSof web-based user interface.

To configure a Service and Policy using the CoroSof user interface

1. Open the CoroSof Administration Console. From the navigation pane, under **Services**, click **Automation** to begin creation of an automated service.

2. Select one of the provided service templates on which to base the new automated service. These templates are created to simplify the service setup.

For example, if you are automating an HTTP service, choose the HTTP template. See the following example of the HTTP template:

Automate Linux_HTTPD (Step 1 of 4)

Set Automation Values for Service Management

Please update the automation configuration values for your service as needed below.

General

AppName: (Unique name of your service (one word))

Desc: (Service Description)

Load Balancer Settings (HTTPD)

This application services real ports and does not use a load balancer

AppRPort: (Real Ports (comma-separated))

This application services virtual IP:ports using a load balancer

LB Type Filter: (Load Balancer Type)

These are the Virtual IP:Port(s) currently handled by your BigIP load balancers.

	Virtual IP:Port	Load Balancer	Persistence Timeout	Connection Type	Delete
<input type="checkbox"/>	192.168.104.115/24:21	192.168.104.113	(off)	NAT	[Delete]
<input type="checkbox"/>	192.168.104.115/24:53	192.168.104.113	(off)	NAT	[Delete]
<input type="checkbox"/>	192.168.104.115/24:80	192.168.104.113	(off)	NAT	[Delete]
[Add BigIP Virtual IP:Port Entry]					

AppVip:

Monitoring

AppStdTest: (Monitor command)

Figure 1.3 The CoroSft HTTP service template.

- The Automate screen displays. This screen lets you specify how the CoroSft Director manages a service.
3. In the **General** section, change the AppName from the template name to one more descriptive of your system. You can type an optional description of the Service, if desired.
 4. Select the option button for **This application services virtual IP:ports using a load balancer**, and choose **BIG-IP** from the list.
 5. A list of virtual server IPs and ports that are currently handled by the BIG-IP system are displayed in the **AppVip:** box:
 - a) If the virtual server IP and port already exist, simply check the box next to the entry you want to use.
 - b) If the virtual server IP and port do not exist, click **Add BIG-IP Virtual IP:Port Entry**, and enter the virtual server IP and port information, as well as whether you want Connection Persistence

on or off. If you want connection persistence, you must specify a number of seconds in the **Timeout** box.

When you are finished, click the **Save** button.

6. In the next sections, you must provide the Director with the information on how to start and stop the service, how to tell if a service is running, how to test the process level on the server, and how to manage traffic to the service. Enter or edit this command information as applicable to your configuration, then click **Next**.
7. A list of all active servers installed with the CoroSoft agent displays. Choose the server(s) that you want to include for this service, then click **Next**. When selected, a checkmark appears beside the server.
8. Enable the server, or verify that the server is already enabled, for the service. When enabled, a checkmark appears beside the server. Only enable the automation for servers on which the service has been installed and tested.
9. As you have just configured the Service in the steps above, the next step is to create the policy. Policies are the heart of the managed system: they can be as simple or as complex as you need. CoroSoft recommends that you begin with as simple a policy as you can have that still meets your needs. As you see how the system resources are used, increase the complexity of the policy rules as needed, adding rules one at a time to ensure that they perform the way you want.

For specific information on configuring policies, refer to the CoroSoft documentation.

When you have completed the configuration, you will find that CoroSoft, through iControl, has automatically created the necessary configuration settings (pool, virtual server, load balancing method, persistence, etc) on the BIG-IP system for Auto Provisioning.

Optimizing the BIG-IP configuration

The following two optional procedures can help you optimize the BIG-IP system for use with the CoroSoft Automation Suite.

For detailed information on configuring the BIG-IP product, see the ***BIG-IP Solutions Guide*** and the ***BIG-IP Reference Guide*** appropriate for the version of the BIG-IP system you are using.

Configuring an optional health monitor

The BIG-IP system has the ability to perform very comprehensive health checks to verify true resource availability. While performing the steps above, a simple ICMP health check is automatically configured, which only determines whether the node is UP or DOWN. You can optionally configure

one of the BIG-IP system's more complex health checks, like the Extended Content Verification (ECV). The ECV monitor goes much further than a standard ICMP health check, by actually using **send** and **recv** statements in an attempt to retrieve explicit content from nodes.

◆ **Tip**

*You can configure ECV or other health monitors for the pool of servers that CoroSofT automatically creates, the optional pool that contains the CoroSofT Director(s) created in the **Defining the pool** section below, or any other pool managed by the BIG-IP system.*

To configure an ECV health monitor using the BIG-IP Configuration utility.

1. In the navigation pane, click **Monitors**.
The Network Monitors screen opens.
2. Click the **Add** button.
The Add Monitor screen opens.
3. In the Add Monitor screen, type the name of your monitor (it must be different from the monitor template name), and in the **Inherits From** box, select a monitor template from the list. Click the **Next** button.
4. In the Configure Basic Properties section, type an Interval and Timeout value. We recommend 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). Click the **Next** button.
5. In the Configure ECV HTTP Monitor section, enter the appropriate information for your configuration.

Important Note:

*If you are using the **GET** send string, you must end the string by including the HTTP protocol at the end of the statement. Use the following syntax:*

GET <fully qualified path name> HTTP/1.0 \n\n

For example:

GET /www/support/customer_info_form.html HTTP/1.0 \n\n

After completing the applicable information, click the **Done** button.

6. In the navigation pane, click **Monitors**.
The Monitors screen opens.
7. Click the tab corresponding to the type of association you want:
 - If you are associating the monitor with a node (the IP address plus the port) click the Node Associations tab.
 - If you are associating the monitor with a node address only (the IP address minus the port), click the Node Address Associations tab.

- If you are associating the monitor with a service only (that is, the service minus the IP address), click the Service Associations tab.
8. Regardless of the selection you made in step 7, a dialog box opens. In the **Choose Monitor** box, select the monitor you created in step 3 from the list.
 9. If you want to associate more than one monitor, click the Move (>>) button to add the monitor name to the **Monitor Rule** box.
 10. Repeat the previous two steps for each monitor you want to associate with a node.
 11. From the list of Nodes, in the **Associate Current Monitor Rule** column, check the box for each server you want to associate with this monitor.
 12. Click the **Apply** button.
For additional information associating a monitor, click the **Help** button.

Configuring an optional pool and virtual server on the BIG-IP system for the CoroSft Director

For an increased level of high availability, you can configure an *optional* virtual server and pool on the BIG-IP system. This *optional* pool/virtual server on the BIG-IP will contain two or more instances of the CoroSft Director, one that is active, and the other(s) as acting as a back up, and is strictly for administration purposes. For example, if the active CoroSft Director goes down, you can connect to the administrative web interface on the back up CoroSft Director through the virtual server on the BIG-IP system, and start it up.

Important

*This procedures below are only for **manually** creating a pool and virtual server on the BIG-IP system. When you originally configure CoroSft to use the BIG-IP system, CoroSft automatically creates a pool and virtual server on the BIG-IP system for Dynamic Provisioning. The following procedure is for creating a pool and virtual server that do not require Dynamic Provisioning, and is for an **optional** pool that contains the CoroSft Director(s).*

Use the following procedures to configure the *optional* pool and virtual server for the CoroSft Director.

Defining the pool

The first step is to define a load balancing pool for the CoroSft Director. You can define a pool from the BIG-IP Configuration utility or the command line.

To create a pool using the BIG-IP Configuration utility

1. Open the BIG-IP web-based Configuration utility.
2. In the navigation pane, click **Pools**.
The Pools screen opens.
3. Click the **Add** button.
The Add Pool screen opens.
4. In the **Pool Name** box, enter a name for your pool. In our example, we use **director_pool**.
5. In the **Load Balancing Method** box, enter a load balancing method. Remember that this pool is not primarily for load balancing, but for high availability, so the load balancing method you choose is not important.
6. In the **Resources** section, you add the CoroSoft Director servers to the pool.
 - a) In the **Member Address** box, type the IP address of the CoroSoft Director. In our example, the IP address we type is **192.168.100.10**.
 - b) In the **Service** box, type the service number you want to use for this node (for example **443**), or specify a service by choosing a service name from the list (for example **https**). In our example, we use **https, 443**.
 - c) Leave the **Member Ratio** box empty, it defaults to **1**.
 - d) In the **Member Priority** box, if you are adding the active CoroSoft Director, type **2** and press Enter.
If you are adding the back up CoroSoft Director, type **1** and press Enter.
 - e) Click the Add button (>>) to add the member to the **Current Members** list.
 - f) Repeat Steps a-e for any other CoroSoft Director instances.
In our example, we repeat the steps once for our back up Director at **192.168.100.11:443**.
7. In the **Minimum Active Member** box, type **1** and press Enter.
8. The other fields in the Add Pool screen are optional. Configure these fields as applicable for your network. (For additional information about configuring a pool, click the **Help** button.)
9. Click the **Done** button.

To define the pool from the command line

To define a pool from the command line, use the following syntax:

```
b pool <pool_name> {member <member_definition> ... member <member_definition>}
```

In our example, the command is:

```
b pool director_pool { \
```

```
member 192.168.100.10:443 \  
member 192.168.100.443 \}
```

Defining the virtual server

The next step is to define a virtual server that references the pool. Again, you can define the virtual server from the BIG-IP Configuration utility or the command line.

To define the virtual servers using the Configuration utility

1. In the navigation pane, click **Virtual Servers**.
The Virtual Servers screen opens.
2. Click the **Add** button.
The Add Virtual Server screen opens.
3. Enter the IP address and service for the virtual server, then click the **NEXT** button. In our example, we use **209.225.33.134** with service of **443**.
The Configure Basic Properties screen displays.
4. On the Configure Basic Properties screen, leave **Enable Address Translation** and **Enable Port Translation** boxes checked. The other fields are optional, configure these fields as applicable to your network. Click the **NEXT** button.
The Select Physical Resources screen displays.
5. Click the **Pool** option button, and from the list, select the pool you created in the *Defining the pool* section above.
6. You can click **Done** or **Next**. If you click the **NEXT** button, you have the option of configuring redundant and outbound properties of the virtual server.
For additional information about configuring a virtual server, click the **Help** button.

To define the virtual servers from the command line

Use the bigpipe virtual command as shown below. You can use standard service names in place of port numbers. If you have DNS configured, you can also use host names in place of IP addresses.

```
b virtual <virt IP>:<port> use pool <pool_name>
```

In our example, we use:

```
b virtual 209.225.33.134:80 use pool director_pool
```