Deployment Guide

nPath Routing

Deploying the BIG-IP System v11 for nPath Routing

What's inside:

Document Version
1.0

Welcome to the F5 deployment guide for nPath routing. This document contains guidance on configuring the BIG-IP system version 11 for nPath (also known as Asymmetric routing or Direct Server Return (DSR)).

BIG-IP version 11.0 introduces iApp™ Application templates, an extremely easy way to accurately configure the BIG-IP system for nPath routing.

To provide feedback on this deployment guide or other F5 solution documents, contact us at *solutionsfeedback@f5.com.*

Products and versions tested

Product	Version
BIG-IP LTM	v11

Important: *Make sure you are using the most recent version of this deployment guide, available at http://www.f5.com/pdf/deployment-guides/npath-iapp-dg.pdf.*

What is nPath routing?

With the nPath routing configuration, you can route outgoing server traffic around the BIG-IP system directly to an outbound router. This method of traffic management increases outbound throughput because packets do not need to be transmitted to the BIG-IP system for translation and forwarding to the next hop.

In bypassing the BIG-IP system on the return path, nPath routing departs significantly from a typical load-balancing configuration. In a typical load-balancing configuration, the destination address of the incoming packet is translated from that of the virtual server to that of the server being load balanced to, which then becomes the source address of the returning packet. A default route set to the BIG-IP system then sees to it that packets returning to the originating client return through the BIG-IP system, which translates the source address back to that of the virtual server.

For more information on nPath routing, see the BIG-IP documentation.

What is F5 iApp™?

New to BIG-IP version 11, F5 iApp is a powerful new set of features in the BIG-IP system that provides a new way to architect application delivery in the data center, and it includes a holistic, application-centric view of how applications are managed and delivered inside, outside, and beyond the data center. The iApp template for nPath acts as the single-point interface for building, managing, and monitoring your nPath deployment.

For more information on iApp, see the White Paper *F5 iApp: Moving Application Delivery Beyond the Network:* *http://www.f5.com/pdf/white-papers/f5-iapp-wp.pdf*.

Prerequisites and configuration notes

The following are general prerequisites and configuration notes for this guide:

- For this deployment guide, the BIG-IP LTM system ***must*** be running version 11.0 or later. If you are using a previous version of the BIG-IP LTM system, see the Deployment Guide index on F5.com. The configuration described in this guide does not apply to previous versions.

- This deployment guide provides guidance for using the iApp for nPath found in version 11.0 and later. For advanced users extremely familiar with the BIG-IP, there is a manual configuration table at the end of this guide. However, we strongly recommend using the iApp template.

Preparation Worksheet

In order to use the iApp for nPath routing, you need to gather some information, such as server IP addresses and domain information. Use the following worksheet to gather the information you will need while running the template. The worksheet does not contain every question in the template, but rather includes the information that is helpful to have in advance. More information on specific template questions can be found on the individual pages.

You might find it useful to print this table and then enter the information.

➲ **Note:** *Although we show space for 10 pool members, you may have more or fewer members in each pool.*

IP Addresses/Port	Protocol	Pool Members	Sync/Failover Groups*	Persistence	Idle Timeout
IP address you will use for the LTM virtual server: Port for this virtual server:	Which protocol do you want to use for nPath routing? The choices are: TCP UDP All Protocols	Server IP addresses: 1: 2: 3: 4: 5: 6: 7: 8: 9: 10: Port used by the servers:	If using the Advanced feature of Sync/Failover Groups, you must already have a Device Group and a Traffic Group Device Group name: Traffic Group name:	Do you want to connections to persist to the same server after the initial connection?	Timeout for unused connections (51 seconds is the default):
Monitor Type					
Which monitor type do you want to use to check the health of the servers? The choices are: ICMP TCP UDP					

** Optional*

Configuring the BIG-IP iApp for nPath

Use the following guidance to help you configure the BIG-IP system for nPath routing using the BIG-IP iApp template.

Getting Started with the iApp for nPath

To begin the nPath iApp Template, use the following procedure.

1. Log on to the BIG-IP system.
2. On the Main tab, expand **iApp**, and then click **Application Services**.
3. Click **Create**. The Template Selection page opens.
4. In the **Name** box, type a name. In our example, we use **nPath_**.
5. From the **Template** list, select **f5.npath**.
   The nPath template opens.

Advanced options

If you select Advanced from the Template Selection list, you see Sync and Failover options for the application. This feature, new to v11, is a part of the Device Management configuration. This functionality extends the existing High Availability infrastructure and allows for clustering, granular control of configuration synchronization and granular control of failover. For more information on Device Management, see the Online Help or product documentation.

1. **Configure Sync/Failover?**
   If you want to configure the Application for Sync or failover groups, select **Yes** from the list.
   a. **Device Group**
      If you select Yes from the question above, the Device Group and Traffic Group options appear. If necessary, uncheck the Device Group box and then select the appropriate Device Group from the list.
   b. **Traffic Group**
      If necessary, uncheck the Traffic Group box and then select the appropriate Traffic Group from the list.

Virtual Server Questions

The next section of the template asks questions about the BIG-IP virtual server. A virtual server is a traffic-management object on the BIG-IP system that is represented by an IP address and a service. Clients send application traffic to a virtual server, which then directs the traffic according to your configuration instructions.

1. **IP address for the virtual server**
   This is the address clients use to access the servers (or a FQDN will resolve to this address). You need an available IP address to use here.
2. **Port**
   This is the service port associated with the virtual server. Type a port number.
3. **Protocol**
   Choose the protocol for this virtual server. You can select **TCP**, **UDP**, or ***All Protocols**. If you are unsure, we recommend choosing ***All Protocols**.

4. **Persistence**
   Choose whether you want connections to persist to the same server after the initial connection has been made. If you chose Yes, the BIG-IP system creates a Source Address Affinity persistence profile.
5. **Timeout**
   Type the number of seconds you want to use before the BIG-IP system closes unused connections. The default is 51 seconds.

Server Pool, Load Balancing, and Service Monitor questions

In this section, you add the servers, and configure the health monitor and pool.

1. **New Pool**
   Choose **Create New Pool** unless you have already made a pool on the LTM for the servers.
2. **Load balancing method**
   While you can choose any of the load balancing methods from the list, we recommend the default, **Least Connections (member)**.
3. **Address/Port**
   Type the IP Address and Port for each server. You can optionally add a Connection Limit. Click **Add** to add additional servers to the pool.
4. **Health Monitor**
   Choose **Create New Monitor** unless you have already made a health monitor on the LTM for the servers in this deployment.
5. **Monitor Type**
   Choose the type of health monitor you want to use for the servers in this deployment. You can choose ICMP, TCP or UDP. If you choose TCP or UDP, addition options appear.
6. **Monitor Interval**
   Type how often (in seconds) you want the BIG-IP system to check the health of the servers. The default is every 30 seconds.
7. **Monitor Request string**
   If you chose a TCP or UDP monitor, you have the option of using a unique Send String the BIG-IP system uses to check the health of the servers. You can configure the template to retrieve a specific page by typing the path here. Leaving the default (GET /) marks the node up if anything is returned from the web page.

   If you chose an ICMP monitor, this option does not appear.
8. **Monitor Response string**
   If you configured a unique HTTP Request, this is where you enter the expected response.

   If you chose an ICMP monitor, this option does not appear.

Finished

Review the answers to your questions. When you are satisfied, click the **Finished** button. The BIG-IP system creates the relevant objects for the nPath implementation.

Next steps

After completing the iApp Template, the BIG-IP Application Services page opens for the nPath service you just created. To see the list of all the configuration objects created to support the nPath deployment, on the Menu bar, click **Components**. The complete list of all nPath related objects opens. You can click individual objects to see the settings.

Once the objects have been created, you are ready to use the new deployment.

Modifying DNS settings to use the BIG-IP virtual server address

Before sending traffic to the BIG-IP system, your DNS administrator may need to modify any DNS entries for the nPath implementation to point to the BIG-IP system's virtual server address.

Modifying the iApp configuration

The iApp application service you just created can be quickly and easily modified if you find it necessary to make changes to the configuration. The Strict Updates feature of the iApp prevents users from manually modifying the iApp configuration (Strict Updates can be turned off, but use extreme caution). As a safer option, the iApp allows you to re-enter the template, make changes, and then update the template. The modifications are automatically made to any of the associated objects.

To modify the configuration

1. On the Main tab, expand **iApp** and then click **Application Services**.
2. Click the name of your nPath Application Service from the list.
3. On the Menu bar, click **Reconfigure**.
4. Make the necessary modifications to the template.
5. Click the **Finished** button.

Viewing statistics

You can easily view a number of different statistics on the BIG-IP system related to the nPath configuration objects created by the iApp template.

Object-level statistics
Use the following procedure to view object-level statistics.

To view object-level statics

1. On the Main tab, expand **Overview**, and then click **Statistics**.
2. From the **Statistics Type** menu, you can select **Virtual Servers** to see statistics related to the virtual servers.
3. You can also choose **Pools** or **Nodes** to get a closer look at the traffic.
4. To see Networking statistics in a graphical format, click **Dashboard**.

For more information on viewing statistics on the BIG-IP system, see the online help or product documentation.

Appendix: Manual configuration table

We strongly recommend using the iApp template to configure the BIG-IP system for nPath. Advanced users extremely familiar with the BIG-IP system can use the following table to manually configure the BIG-IP system.

The following table contains a list of BIG-IP LTM configuration objects along with any non-default settings you should configure as a part of this deployment. Unless otherwise specified, settings not mentioned in the table can be configured as applicable for your configuration. For specific instructions on configuring individual objects, see the online help or product manuals.

BIG-IP LTM Object	Non-default settings/Notes		
Health Monitor (*Main tab-->Local Traffic -->Monitors*) Choose one	***ICMP***	***Name***	Type a unique name
		Type	**ICMP**
		Interval	**30** (recommended)
		Timeout	**91** (recommended)
	TCP	***Name***	Type a unique name
		Type	**TCP**
		Interval	**30** (recommended)
		Timeout	**91** (recommended)
	UDP	***Name***	Type a unique name
		Type	**UDP**
		Interval	**30** (recommended)
		Timeout	**91** (recommended)
Pool (*Main tab-->Local Traffic -->Pools*)	***Name***	Type a unique name	
	Health Monitor	Select the monitor you created above	
	Slow Ramp Time[1]	**300**	
	Load Balancing Method	Choose a load balancing method. We use the default **Round Robin**	
	Address	Type the IP Address of the nodes	
	Service Port	Choose the appropriate port (click **Add** to repeat Address and Service Port for all nodes)	
Profiles (*Main tab-->Local Traffic -->Profiles*)	***Fast L4*** (*Profiles-->Protocol*)	Name	Type a unique name
		Parent Profile	**Fast L4**
		Idle Timeout	**51** (recommended)
		Loose Close	**Enabled**
		TCP Close Timeout	**51** (recommended)
	Persistence[2] (*Profiles-->Persistence*)	Name	Type a unique name
		Persistence Type	**Source Address Affinity**
Virtual Servers (*Main tab-->Local Traffic -->Virtual Servers*)	***Name***	Type a unique name	
	Address	Type the IP Address for the virtual server	
	Service Port	Choose the appropriate port	
	Type	**Performance (Layer 4)**	
	Protocol	Select the appropriate protocol (**TCP**, **UDP**, or ***All Protocols**)	
	Protocol Profile (client)[1]	Select the Fast L4 profile you created above	
	Default Pool	Select the pool you created above	
	Persistence Profile	Select the Persistence profile you created above	

[1] You must select **Advanced** from the **Configuration** list for these options to appear
[2] Only necessary if you require persistence to the same server after a connection has been made

Document Revision History

Version	Description
1.0	New Version

F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 www.f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com