Deploying the BIG-IP System for Microsoft Application Virtualization

Welcome to the F5 and Microsoft Application Virtualization deployment guide. Use this document for guidance on configuring the BIG-IP system version 11 and later to provide performance and availability for App-V 5.0 SP2 Publishing and Management servers. When configured according to the instructions in this guide, the BIG-IP system performs as a reverse proxy for App-V.

F5 provides high availability and intelligent health monitoring for App-V services such as Management, Publishing, SMB, and HTTP Streaming servers.

Products and applicable versions

Product	Version
BIG-IP LTM	11.0 - 11.6
Microsoft Application Virtualization (App-V)	5.0 SP2
Deployment guide version	1.0

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

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

Contents

Prerequisites and configuration notes

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

- The BIG-IP system must be running BIG-IP version 11.0 or later, and all initial configuration tasks must be complete.
- You must have DNS A records pointing Publishing, Management, file share, and streaming FQDNs to their respective BIG-IP virtual server addresses.
- When importing sequenced packages, use the FQDNs/file share names specified above in the HTTP/UNC path.
- If you are configuring SSL Bridging for HTTP Streaming traffic, you must have obtained the appropriate SSL certificate and key, and installed them on the BIG-IP LTM system. See System > File Management > SSL Certificate list. Refer to the Help tab or the BIG-IP documentation for specific instructions on importing certificates.

Configuration example

The following diagram shows a logical configuration diagram with the BIG-IP system providing high availability and intelligent health monitoring for a Microsoft App-V deployment. It also shows the optional Direct Server Return (nPath) configuration that is described in *Optional: Configuring Direct Server Return for SMB Traffic on page 8.*

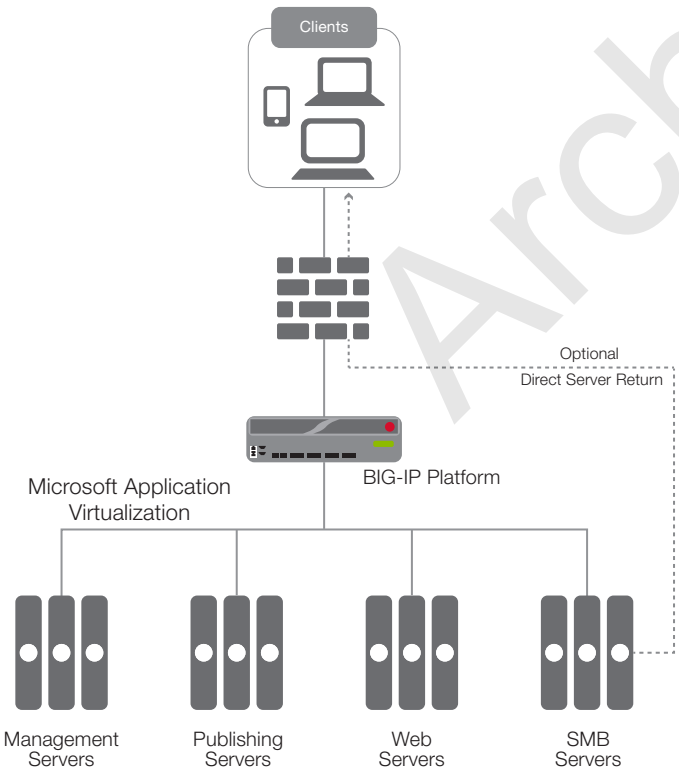

Figure 1: *Logical configuration example*

Configuring the BIG-IP LTM for Microsoft App-V

Use the following tables for guidance on configuring the BIG-IP system for the Microsoft Application Virtualization. These tables contains any non-default setting you should configure as a part of this deployment. Settings not contained in the table can be configured as applicable. For specific instructions on configuring individual objects, see the online help or product manuals.

Publishing Server configuration table

Use this table for configuring the BIG-IP system for the Publishing server.

BIG-IP object	Non-default settings/Notes		
Health Monitor (*Local Traffic-->Monitors*)	***Name***	Type a unique name	
	Type	**HTTP**	
	Interval	**30**	
	Timeout	**91**	
	Send String[1,2]	**GET / HTTP/1.1\r\nHost: publish.example.local\r\n**	
	Receive String[1]	**Publishing**	
	User Name[1]	Type a user name with access to the implementation	
	Password[1]	Type the associated password	
Pool (*Local Traffic -->Pools*)	***Name***	Type a unique name	
	Health monitor	Add health monitor above	
	Load Balancing Method	**Least Connections (member)** recommended	
	Address	IP address of a Publishing Server	
	Service Port	**8081** Repeat Address and Port for all members	
Profiles (*Local Traffic-->Profiles*)	***HTTP*** (*Profiles-->Services*)	Name	Type a unique name
		Parent Profile	**http**
	TCP WAN (*Profiles-->Protocol*)	Name	Type a unique name
		Parent Profile	**tcp-wan-optimized**
		Idle Timeout	**1800**
	TCP LAN (*Profiles-->Protocol*)	Name	Type a unique name
		Parent Profile	**tcp-lan-optimized**
		Idle Timeout	**1800**
	Persistence (*Profiles-->Persistence*)	Name	Type a unique name
		Persistence Type	**Source Address Affinity**
		Idle Timeout	**1800**
Virtual Server (*Local Traffic-->Virtual Servers*)	***Name***	Type a unique name	
	Destination Address	IP address for the virtual server	
	Service Port	**8081**	
	Protocol Profile (Client)[1]	Select the TCP WAN profile you created above	
	Protocol Profile (Server)[1]	Select the TCP LAN profile you created above	
	HTTP Profile	Select the HTTP profile you created above	
	Source Address Translation	**Auto Map** (SNAT is recommended. If you expect more than 64,000 concurrent connections per server, use a SNAT Pool[2] instead of Auto Map)	
	Default Pool	Select the pool you created above	
	Default Persistence Profile	Select the persistence profile you created above	

[1] *You must select* **Advanced** *from the* **Configuration** *list for these options to appear.*
[2] *For more information on SNAT Pools, see the BIG-IP documentation*

Management Server configuration table

Use the following guidance for configuring the BIG-IP system for the Management server.

BIG-IP object	Non-default settings/Notes	
Health Monitor (*Local Traffic-->Monitors*)	***Name***	Type a unique name
	Type	**HTTP**
	Interval	**30**
	Timeout	**91**
	Send String[1,2]	**GET /Console.html HTTP/1.1\r\nHost: manage.example.local\r\n**
	Receive String[1]	**200 OK**
	User Name[1]	Type a user name with access to the implementation
	Password[1]	Type the associated password
Pool (*Local Traffic -->Pools*)	***Name***	Type a unique name
	Health monitor	Add health monitor above
	Slow Ramp Time[1]	**300**
	Load Balancing Method	**Least Connections (member)** recommended
	Address	IP address of a Management Server
	Service Port	**8080** Repeat Address and Port for all members
Profiles (*Local Traffic-->Profiles*)	***HTTP*** (*Profiles-->Services*)	Name: Type a unique name Parent Profile: **http**
	TCP WAN (*Profiles-->Protocol*)	Name: Type a unique name Parent Profile: **tcp-wan-optimized**
	TCP LAN (*Profiles-->Protocol*)	Name: Type a unique name Parent Profile: **tcp-lan-optimized**
	Persistence (*Profiles-->Persistence*)	Name: Type a unique name Persistence Type: **Source Address Affinity** Idle Timeout: **1800**
Virtual Server (*Local Traffic-->Virtual Servers*)	***Name***	Type a unique name
	Destination Address	IP address for the virtual server
	Service Port	**8080**
	Protocol Profile (Client)[1]	Select the TCP WAN profile you created above
	Protocol Profile (Server)[1]	Select the TCP LAN profile you created above
	HTTP Profile	Select the HTTP profile you created above
	Source Address Translation	**Auto Map** (SNAT is recommended. If you expect more than 64,000 concurrent connections per server, use a SNAT Pool[2] instead of Auto Map)
	Default Pool	Select the pool you created above
	Default Persistence Profile	Select the persistence profile you created above

[1] *You must select* **Advanced** *from the* **Configuration** *list for these options to appear.*
[2] *For more information on SNAT Pools, see the BIG-IP documentation*

SMB configuration table

Use the following guidance for configuring the BIG-IP system for SMB traffic.

If you are configuring the BIG-IP system for Direct Server Return (nPath), see *Configuring the BIG-IP system for Direct Server Return and SMB traffic on page 8* for an additional profile, and an alternate virtual server configuration.

BIG-IP object	Non-default settings/Notes	
Health Monitor (*Local Traffic-->Monitors*)	***Name***	Type a unique name
	Type	**TCP**
	Interval	**30**
	Timeout	**91**
Pool (*Local Traffic -->Pools*)	***Name***	Type a unique name
	Health monitor	Add health monitor above
	Load Balancing Method	**Least Connections (member)** recommended
	Address	IP address of a file share server
	Service Port	**445** Repeat Address and Port for all members
Profiles (*Local Traffic-->Profiles*)	***Persistence*** (*Profiles-->Persistence*)	Name: Type a unique name
		Persistence Type: **Source Address Affinity**
		Idle Timeout: **1800**
Virtual Server (*Local Traffic-->Virtual Servers*)	***Name***	Type a unique name
	Type	**Performance (Layer 4)**
	Destination Address	IP address for the virtual server
	Service Port	**445**
	Source Address Translation	**Auto Map** (SNAT is recommended. If you expect more than 64,000 concurrent connections per server, use a SNAT Pool[2] instead of Auto Map)
	Default Pool	Select the pool you created above
	Default Persistence Profile	Select the persistence profile you created above

[1] *You must select* **Advanced** *from the* **Configuration** *list for these options to appear.*
[2] *For more information on SNAT Pools, see the BIG-IP documentation*

HTTP Streaming configuration table

Use the following table for guidance on configuring the BIG-IP system for HTTP Streaming. If you want the BIG-IP system to perform SSL bridging (where the BIG-IP system unencrypts incoming traffic, and then re-encrypts it before sending it back to the servers), follow the SSL Bridging notes.

BIG-IP object	Non-default settings/Notes		
Health Monitor (*Local Traffic-->Monitors*)	***Name***	Type a unique name	
	Type	**HTTP** (**HTTPS** if you are deploying SSL Bridging)	
	Interval	**30**	
	Timeout	**91**	
	Send String[1,2]	**GET /Content/ HTTP/1.1\r\nHost: publish.example.local\r\n**	
	Receive String[1]	**web.config**	
	User Name[1]	Type a user name with access to the implementation	
	Password[1]	Type the associated password	
Pool (*Local Traffic -->Pools*)	***Name***	Type a unique name	
	Health monitor	Add health monitor above	
	Slow Ramp Time[1]	**300**	
	Load Balancing Method	**Least Connections (member)** recommended	
	Address	IP address of an HTTP streaming content server	
	Service Port	**80** (**443** if you are deploying SSL Bridging) Repeat Address and Port for all members	
Profiles (*Local Traffic-->Profiles*)	***Persistence*** (*Profiles-->Persistence*)	Name	Type a unique name
		Persistence Type	**Source Address Affinity**
		Idle Timeout	**1800**
	Additional profiles if you are configuring SSL bridging		
	Client SSL *(Profiles > SSL)*	Name	Type a unique name
		Parent Profile	**clientssl**
		Certificate and Key	Select the Certificate and Key you imported from the associated list
	Server SSL *(Profiles > Other)*	Name	Type a unique name
		Parent Profile	**serverssl**
Virtual Server (*Local Traffic-->Virtual Servers*)	***Name***	Type a unique name	
	Type	**Performance (Layer 4)** (**Standard** if you are deploying SSL Bridging)	
	Destination Address	IP address for the virtual server	
	Service Port	**80** (**443** if you are deploying SSL Bridging)	
	Source Address Translation	**Auto Map** (SNAT is recommended. If you expect more than 64,000 concurrent connections per server, use a SNAT Pool[2] instead of Auto Map)	
	Default Pool	Select the pool you created above	
	Default Persistence Profile	Select the persistence profile you created above	

[1] *You must select* **Advanced** *from the* **Configuration** *list for these options to appear.*
[2] *For more information on SNAT Pools, see the BIG-IP documentation*

Optional: Configuring Direct Server Return for SMB Traffic

In traditional load balancing implementations, both incoming client traffic and the return server traffic flow through the BIG-IP system. With Direct Server Return (DSR), or nPath, the incoming client traffic flows through the BIG-IP device and to the application server, however the return traffic is routed around the BIG-IP system and sent directly to the client. Because App-V relies on protocols that use a simple request-in and large-stream-back model, this architecture has the benefit of eliminating the impact that the large amount of streaming traffic would have on your BIG-IP system.

App-V Server Configuration

To support the deployment of DSR/nPath, you must configure a loopback adapter with the SMB BIG-IP virtual server IP address, and enable **WeakHostReceive** and **Forwarding** on the network interfaces.

Configure the Loopback Adapter

1. From Control Panel, select **Device Manager**.
2. Right-click the computer name and click **Add Legacy Hardware**.
3. Click **Next > Install the hardware that I manually select from a list > Network Adapters > Microsoft > Microsoft Loopback Adapter (Windows 2008 R2)** or **Microsoft KM-TEST Loopback Adapter (Windows 2012/R2)**.
4. When the adapter is successfully installed, configure the IP address of the loopback adapter to match the destination IP address of the BIG-IP virtual server you created for SMB access, with a subnet mask of **255.255.255.255**.
5. You must use Microsoft Windows PowerShell to enable the network interfaces for **WeakHostReceive** and **Forwarding**. From each Windows Server, open Windows PowerShell and run the following commands:
   - **`Get-NetIPInterface`**
     This command lists the server network interfaces. Note the **ifIndex** property of the loopback interface, as well as the interface that corresponds to the port 445 pool member in LTM.
   - **Set-NetIPInterface –InterfaceIndex 1 –WeakHostReceive Enabled –Forwarding Enabled**
     Run this command for each interface you identified above, using the **ifIndex** number for the **–InterfaceIndex** value.

Configuring the BIG-IP system for Direct Server Return and SMB traffic

Use the following guidance for an additional profile and an alternate virtual server configuration.

BIG-IP object	Non-default settings/Notes		
Profiles (*Local Traffic-->Profiles*)	***Fast*** (*Profiles-->Protocol-->FastL4*)	Name	Type a unique name
		Loose Close	**Enabled**
		Idle Timeout	**1800**
Virtual Server (*Local Traffic-->Virtual Servers*)	***Name***	Type a unique name	
	Type	**Performance (Layer 4)**	
	Destination Address	IP address for the virtual server	
	Service Port	**445**	
	Protocol Profile (Client)	Select the Fast L4 profile you created above	
	Source Address Translation	**None**	
	Address Translation	**Disabled**	
	Port Translation	**Disabled**	
	Default Persistence Profile	Select the persistence profile you created in the table on page 6	

Additional information about Direct Server Return/nPath can be found in the following guide:
https://support.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/ltm-implementations-11-1-0/6.html.

Document Revision History

Version	Description	Date
1.0	New guide	10-29-2014

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