

Deployment Guide

IBM WebSphere 8.0



TABLE OF CONTENTS

1 Introduction 4

2 Deployment Guide Overview 4

3 Deployment Guide Prerequisites 4

4 Accessing the AX Series ADC 5

5 IBM WebSphere Application Server Installation Procedures 6

6 Architecture Overview 8

7 Basic Configuration 8

8 Health Monitor Configuration 9

9 Source NAT Configuration 9

10 Server Configuration 10

11 Service Group Configuration 11

12 Virtual Server Configuration 13

 12.1 Validating the Configuration 14

13 Advanced Configuration 15

14 Health Monitoring 15

15 Optional: IBM WebSphere Simple URL Redirect 17

16 Preparing the Configuration 18

 16.1 Add a New Service Type HTTPS 19

 16.2 Import SSL Cert or Create Self-Signed CA 19

 16.2.1 Option 1: Generate a Self-Signed Certificate 19

 16.2.2 Option 2: Import The Certificate and Key 21

 16.3 Create Client-SSL Template and Enable SSL Offload 21

17 HTTP/HTTPS Compression 23

 17.1 Create HTTP Compression Template 23

18	Persistence.....	24
19	Connection Reuse.....	25
20	RAM Caching.....	26
21	Apply Optimization and Acceleration Feature Templates on VIP.....	27
22	Summary and Conclusion.....	28
A.	CLI Commands for Sample Basic Configuration.....	28
B.	CLI Commands for Sample Advanced Configuration.....	29

1 INTRODUCTION

IBM WebSphere 8.0 is one of the leading enterprise middleware application servers for application development and integration software in the market. WebSphere has been on the market since 1998 and is deemed one of the best software applications for on-demand business; WebSphere delivers business integration, application and transaction infrastructure, and portals.

2 DEPLOYMENT GUIDE OVERVIEW

This deployment guide illustrates how an AX series Application Delivery Controller (ADC) can be installed to front-end an IBM WebSphere 8.0 Web Application Server farm infrastructure. This deployment guide utilizes the IBM WebSphere V8 Application Server Network Deployment.

IBM recommends using the WebSphere Network Deployment installer, as it is the only installer and version that can support front-end load balancing. The AX Series ADC offers additional security, reliability and optimization; namely: HTTP Compression, RAM Caching, SSL Offload and HTTP Connection Reuse.

For additional overview information about WebSphere features, please see:

<http://www-01.ibm.com/software/webservers/appserv/was/features/>

For additional information about the IBM WebSphere Network Deployment features and capabilities, please see the following page:

<http://www.ibm.com/developerworks/downloads/ws/wasnetwork/>

3 DEPLOYMENT GUIDE PREREQUISITES

This deployment guide has the following prerequisites:

AX Series Requirement

The A10 Networks AX Series ADC must be running version 2.4.x or higher.

IBM WebSphere Requirements

For IBM requirements please see the following page:

<http://www-01.ibm.com/support/docview.wss?uid=swg27021246>

Tested environment:

- IBM WebSphere V8.0.0.2 Network Deployment (Distributed Platforms)

- ◆ Windows 2008 (64-bit) Enterprise Edition Server Operating System (OS)
- Client Access (tested)
 - ◆ Microsoft Internet Explorer Version 8.0
 - ◆ Google Chrome Version 10.0
 - ◆ Mozilla Firefox Version 8

Note: Generally, if the Virtual IP (VIP) is accessed from an external client, the AX device would be deployed in a routed mode. If the web site services are accessed internally, the AX device would be deployed in one-arm mode. If the web server applications are accessed from both internal and external clients, the AX device would be deployed in one-arm mode.

Note: For additional deployment modes the AX Series device can support, please see the following page:

<http://www.a10networks.com/products/axseries-load-balancing101.php>

4 ACCESSING THE AX SERIES ADC

This section describes how to access the AX Series device. The AX device can be accessed either from a Command Line Interface (CLI) or Graphical User Interface (GUI):

- CLI – Text-based interface in which you type commands on a command line. You can access the CLI directly through the serial console or over the network using either of the following protocols:
 - ◆ Secure protocol – Secure Shell (SSH) version 2
 - ◆ Unsecure protocol – Telnet (if enabled)
- GUI – Web-based interface in which you click to access configuration or management pages and type or select values to configure or manage the device. You can access the GUI using the following protocol:
 - ◆ Secure protocol – Hypertext Transfer Protocol over Secure Socket Layer (HTTPS)

Note: HTTP requests are redirected to HTTPS by default on the AX device.

Default Access Information:

- Default Username: “admin”
- Default Password: “a10”
- Default IP Address of the device: “172.31.31.31”

(For detailed information on how to access the AX Series device, refer to the *A10 Networks AX Series System Configuration and Administration Guide*.)

5 IBM WEBSHERE APPLICATION SERVER INSTALLATION PROCEDURES

This deployment guide is based on Windows 2008 Server IBM WebSphere Network Deployment installation. This deployment guide assumes that the WebSphere servers have been installed and the sites can be accessed directly.

To verify that the WebSphere servers are installed within a cluster:

1. Navigate to the **Servers > Clusters > WebSphere Integration Solution Console**.
2. Click on **WebSphere Application Server Cluster**.
3. On the main frame, click on the cluster name ("a10cluster" in this example).



Figure 1: IBM WebSphere console

4. Click on **Local Topology** from the menu tab and collapse the a10cluster cell as shown in the example below.
5. Collapse the (+) and make sure that the nodes within the clusters are available and services have started.

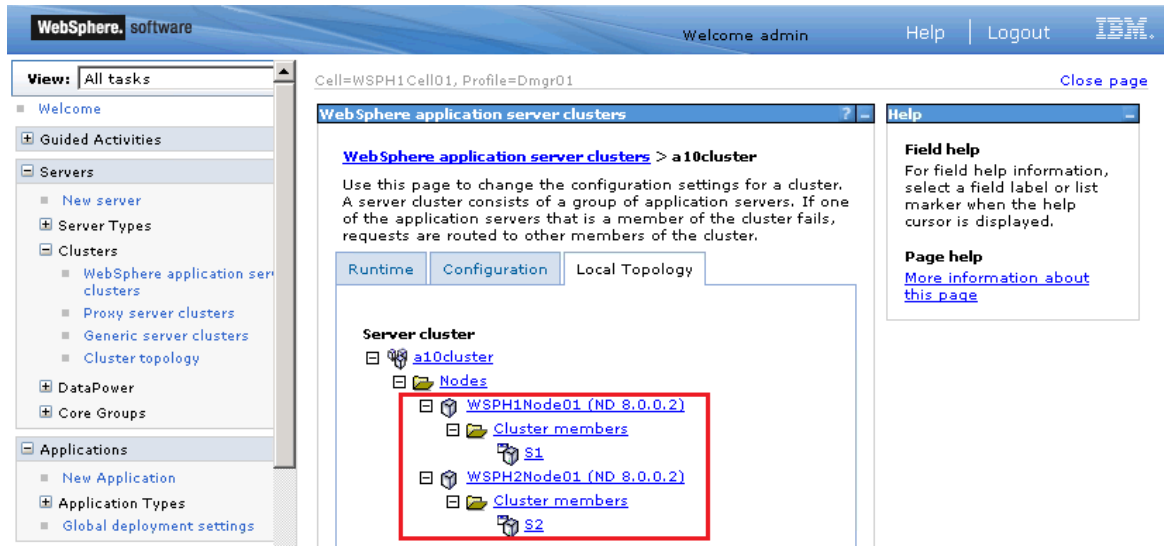


Figure 2: WebSphere admin console

6. To ensure that the IBM WebSphere servers are running, open a browser and navigate directly to the server. As an example, navigate to the following URL: "http://localhost:9080/"
7. Verify that all WebSphere servers are accessible and in functional condition. Once the verification is complete, you can implement the ADC within your IBM WebSphere topology.

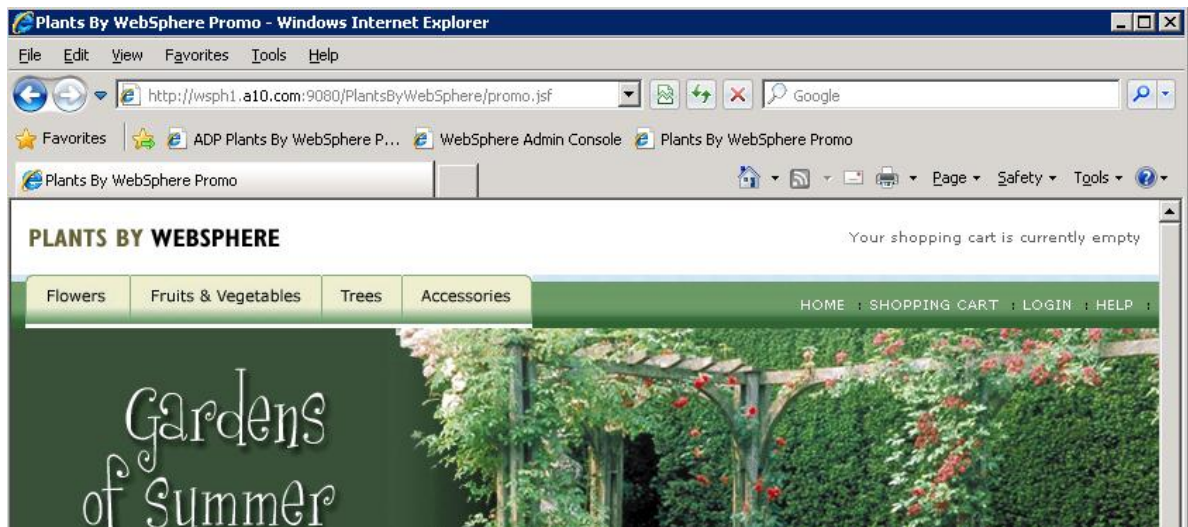


Figure 3: WebSphere sample application

6 ARCHITECTURE OVERVIEW

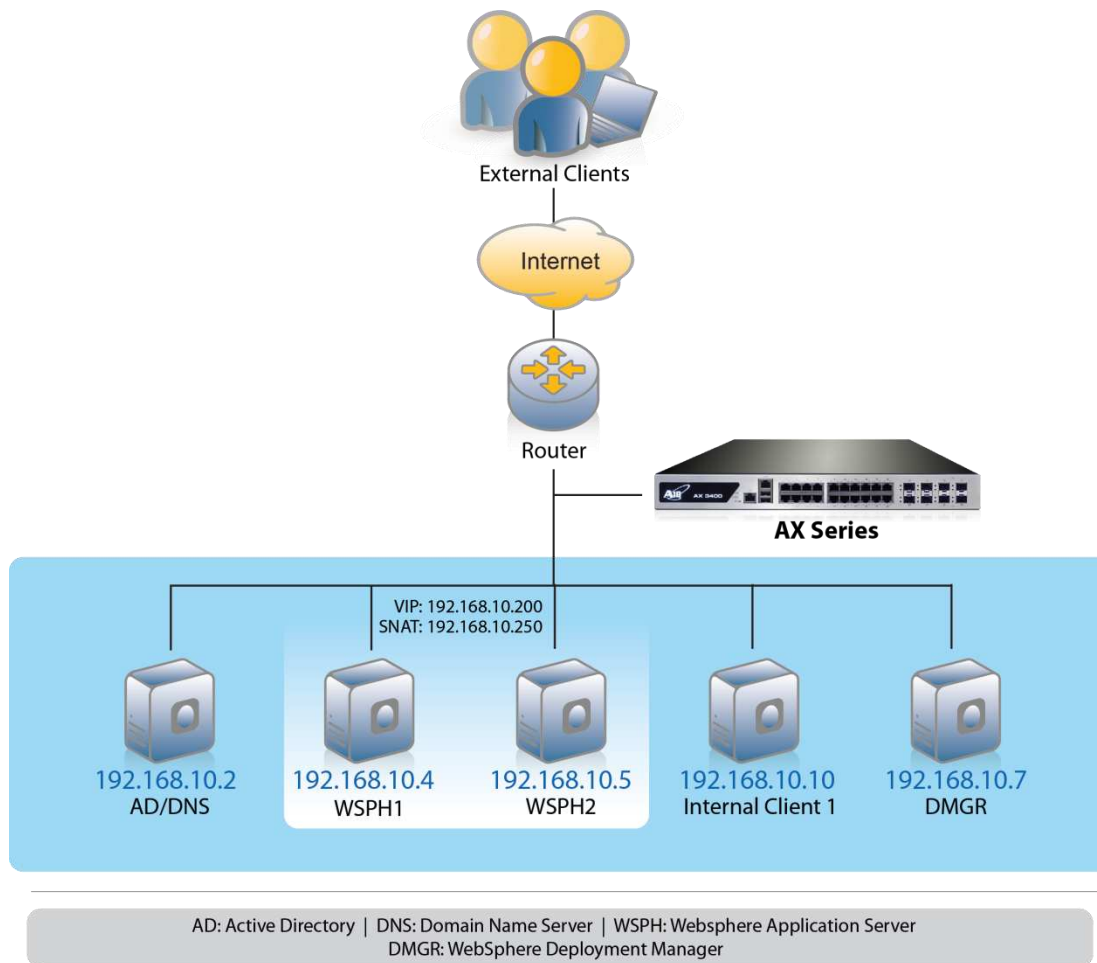


Figure 4: Architecture overview

7 BASIC CONFIGURATION

This section explains how the AX Series is configured with IBM WebSphere V8 Network Deployment. This section contains detailed instructions for installing the real servers, service group, virtual servers, and virtual services for a basic IBM WebSphere web server.

In the basic AX configuration, basic health monitoring is implemented using ICMP pings. In the advanced section of this deployment guide, instructions are provided for deploying an HTTP health monitor.

The basic configuration provides simple load balancing of IBM WebSphere servers using the round robin algorithm. The basic configuration will be deployed in one-arm mode, with external and internal users. Source NAT will be required within this configuration.

8 HEALTH MONITOR CONFIGURATION

The AX series can automatically initiate health status checks for real servers and service ports. Health checks assure that all requests go to functional and available servers. If a server or a port does not respond appropriately to a health check, the server is temporarily removed from the list of available servers. Once the server is restored and starts responding appropriately to the health checks, the server is automatically added back to the list of available servers.

1. Navigate to **Config Mode > Service > Health Monitor**.
2. Click **Add** from the **Health Monitor** drop-down list.
3. In the **Name** field, enter “wshc”.
4. Select **Method** “ping”.
5. Click **OK**, and then see the next section to continue with the Service Group configuration.

<input type="checkbox"/>	Name	Type	Retry	Consec Pass Req'd	Interval(Seconds)	Timeout(Seconds)
<input type="checkbox"/>	ping	ICMP	3	1	5	5

Figure 5: Health monitor configuration

Note: Ping is the default health monitor within the AX Series. Whenever a server is configured on the AX Series, a ping health monitor is configured automatically.

9 SOURCE NAT CONFIGURATION

This section configures the IP Address pool to be used for IP Source Network Address Translation (SNAT). When incoming traffic from a client accesses the VIP address (for example: 10.0.0.200), the client requests are “source NAT-ed”, which means that the AX device replaces the client’s source IP address with an address from a pool of source NAT addresses. SNAT is required when your network topology is based on “one-arm” deployment and if you have internal clients that reside on the same subnet as the VIP.

To configure SNAT, use this section to configure the address pool. Then, later in this document, a procedure shows how to apply the pool to the VIP.

1. Navigate to **Config Mode > Service > IP Source NAT > IPv4 Pool**.

2. Click **Add**.
3. Enter the following:
 - ◆ **NAT:** "WSSNAT"
 - ◆ **Start IP Address:** "192.168.10.225"
 - ◆ **End IP Address:** "192.168.10.225"
 - ◆ **Netmask:** "255.255.255.0"

IPv4 Pool	
Name: *	WSSNAT
Start IP Address: *	192.168.10.225
End IP Address: *	192.168.10.225
Netmask: *	255.255.255.0
Gateway:	
HA Group:	

Figure 6: Source NAT pool configuration

4. Click **OK**, then click **Save** to save the configuration.

Note: When you are in the Virtual Service configuration section, you can apply the SNAT pool to the VIP.

Note: When using the AX device in a High Availability (HA) configuration, an HA group must be selected. This will prevent duplicate IP addresses from occurring in the SNAT Pool.

10 SERVER CONFIGURATION

This section demonstrates how to configure the WebSphere web servers on the AX Series.

1. Navigate to **Config Mode > Service > SLB > Server**.
2. Click **Add** to add a new server.
3. Within the Server section, enter the following required information:
 - ◆ **Name:** "wsph1"
 - ◆ **IP address /Host:** "192.168.10.3"

Note: Enter additional servers if necessary.

General	
Name: *	wsph1
IP Address/Host: *	192.168.10.3 <input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
GSLB External IP Address:	
Weight:	1
Health Monitor:	(default)
Status:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Connection Limit:	8000000 <input checked="" type="checkbox"/> Logging
Connection Resume:	
Slow Start:	<input type="checkbox"/>
Spoofing Cache:	<input type="checkbox"/>
Stats Data:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Extended Stats:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Server Template:	default
Description:	

Figure 7: Server configuration

4. To add a port to the server configuration:
 - a. Enter the port number in the **Port** field.
 - b. Select the **Protocol**.
 - c. Click **Add**.

Port	
Port: *	9080
Protocol:	TCP
Weight(W): *	1
<input type="checkbox"/> No SSL	
Connection Limit(CL):	8000000 <input checked="" type="checkbox"/> Logging
Connection Resume(CR):	
Server Port Template(SPT):	default
Stats Data(SD):	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Health Monitor(HM):	<input checked="" type="radio"/> (default) <input type="radio"/> Follow Port: <input type="text"/> TCP
Extended Stats(ES):	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
<input checked="" type="button" value="Add"/> <input type="button" value="Update"/> <input type="button" value="Delete"/> <input type="button" value="Enable"/> <input type="button" value="Disable"/>	

Figure 8: Server port configuration

5. Click **OK**, then click **Save** to save the configuration.

11 SERVICE GROUP CONFIGURATION

This section shows how to configure a service group.

1. Navigate to **Config Mode > Service > SLB > Service Group**.
2. Click **Add**.

3. Enter or select the following values:
 - ◆ **Name:** "SGWS"
 - ◆ **Type:** "TCP"
 - ◆ **Algorithm:** "Round Robin"
 - ◆ **Health Monitor:** "ping"
4. In the Server section, select a server from the Server drop-down list and enter "9080" in the **Port** field.
5. Click **Add**. Repeat for each server.

Service Group	
Name:	SGWS
Type:	TCP
Algorithm:	Round Robin
Health Monitor:	ping
Min Active Members:	<input type="checkbox"/>
<input type="checkbox"/>	Send client reset when server selection fails
Stats Data:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Extended Stats:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Description:	<input type="text"/>

Figure 9: Service group configuration

Server													
IPv4/IPv6:	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6												
Server:	wsph1												
Server Port Template(SPT):	default												
Port:	9080												
Priority:	1												
Stats Data:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled												
<table border="1"> <thead> <tr> <th><input type="checkbox"/></th> <th>Server</th> <th>Port</th> <th>SPT</th> <th>Priority</th> <th>Stats Data</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/></td> <td>wsph1</td> <td>9080</td> <td>default</td> <td>1</td> <td><input checked="" type="checkbox"/></td> </tr> </tbody> </table>		<input type="checkbox"/>	Server	Port	SPT	Priority	Stats Data	<input checked="" type="checkbox"/>	wsph1	9080	default	1	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Server	Port	SPT	Priority	Stats Data								
<input checked="" type="checkbox"/>	wsph1	9080	default	1	<input checked="" type="checkbox"/>								
<input checked="" type="button" value="Add"/> <input type="button" value="Update"/> <input type="button" value="Delete"/> <input checked="" type="button" value="Enable"/> <input type="button" value="Disable"/>													

Figure 10: Server configuration

6. Click **OK**, then click **Save** to save the configuration.

12 VIRTUAL SERVER CONFIGURATION

This section contains the basic configuration for a Virtual Server. The Virtual Server is also known as the "Virtual IP" ("VIP") that a client accesses during an initial request.

1. Navigate to **Config Mode > Service > SLB > Virtual Service**.
2. In the General section, enter the name of the VIP and its IP address:
 - ◆ **Name:** "wsphvip"
 - ◆ **IP Address:** "192.168.10.200"

General	
Name: *	<input type="text" value="wsphvip"/> <input type="checkbox"/> Wildcard
IP Address or CIDR Subnet: *	<input type="text" value="192.168.10.200"/> <input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
Status:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
ARP Status:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Stats Data:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Extended Stats:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
When-All-Ports-Down:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Redistribution Flagged:	<input type="checkbox"/>
HA Group:	<input type="text"/>
Virtual Server Template:	default
PBSLB Policy Template:	<input type="text"/>
Description:	<input type="text"/>

Figure 11: Virtual server configuration

3. In the Port section, click **Add**.

Virtual Server Port	
Virtual Server:	wsphvip
Type: *	HTTP
Port: *	80
Service Group:	SGWS
Connection Limit:	<input type="checkbox"/> 8000000 <input checked="" type="radio"/> Drop <input type="radio"/> Reset <input checked="" type="checkbox"/> Logging
<input checked="" type="checkbox"/>	Use default server selection when preferred method fails
<input type="checkbox"/>	Use received hop for response
<input type="checkbox"/>	Send client reset when server selection fails

Figure 12: Virtual-server port configuration

4. Select the following values:

- ◆ **Virtual Server:** "HTTP"

Note: The Port number will be pre-selected after selecting the protocol type.

- ◆ **Service Group:** "SGWS"

5. Click **OK**, then click **Save** to save the configuration.

12.1 VALIDATING THE CONFIGURATION

To validate that the IBM WebSphere basic load balancing configuration is functional, you can access the VIP with a browser and type the URL as <http://192.168.10.200> (in this example).

Within the AX GUI, you can validate that the IBM WebSphere back-end (WebSphere) servers are receiving requests from users. Navigate to **Monitor Mode > Service > SLB**.

Name	IName	Connections		Packets		Bytes	
		Current	Total	Forward	Reverse	Forward	Reverse
<input type="checkbox"/>	wsph2/192.168.10.4	3	47	1.7K	2.2K	583.9K	1.9M
<input type="checkbox"/>	TCP/9080	3	47	1.7K	2.2K	583.9K	1.9M
<input type="checkbox"/>	wsph1/192.168.10.3	3	15	145	190	39.7K	134.9K
<input type="checkbox"/>	TCP/9080	3	15	145	190	39.7K	134.9K

Figure 13: Server list

In addition, you also can navigate to **Config Mode > Service > SLB > Virtual Server**.

Name	IP Address or CIDR Subnet	Status	Health	HA Group
wsphvip	192.168.10.200	✓	↑	

Figure 14: Virtual server

Name	Type	Port	IP Address or CIDR Subnet	Status	Health	HA Group
_192.168.10.200_HTTP_9080	HTTP	9080	192.168.10.200	✓	↑	

Figure 15: Virtual services

Name	IP Address/Host	Health Monitor	Status	Health
wsph1	192.168.10.3	ping	✓	↑
wsph2	192.168.10.4	ping	✓	↑

Select All Unselect All Selected: 0

Figure 16: Server list

13 ADVANCED CONFIGURATION

This section of the deployment guide contains the advanced configuration of the AX Series with IBM WebSphere Application Servers. These features can be deployed individually or in combination, with no restrictions. The most common acceleration features that can be used in IBM WebSphere deployments are SSL Offload, HTTP Compression, HTTP Connection Reuse, Cookie Persistence, and RAM Caching. These features increase server performance and provide scalability to the existing back-end WebSphere servers.

The first step in the advanced configuration is to predefine all the optimization and performance features in configuration templates. Once all the performance features are defined in the templates, you can bind the features to the Virtual Server or VIP.

Note: With the assumption that you already understand basic configuration of the server, service group, virtual service and virtual server, this section will move directly to advanced configuration with minimal changes from the basic configuration.

14 HEALTH MONITORING

As mentioned in the Basic AX configuration, the AX Series offers multiple options to monitor the health of a WebSphere application. This section describes what needs to be changed from the Basic to Advanced configuration.

In the Basic AX configuration, a default ping health monitor is used. The Advanced Configuration uses an HTTP health monitor instead. The health monitor needs to be changed on the Server and Service Group configuration pages of the AX Series Graphical User Interface (GUI) as shown in Figure 18 and Figure 19. But before the HTTP health monitor is applied to the Server and Service Group, the HTTP health monitor template must be created.

1. Navigate to **Config Mode > Service > Health Monitoring**.
2. Click **Add**.
3. Name the health monitor template "wshc".

Note: Use the default retry, interval and timeout values unless your deployment has specific requirements to change them.

4. In the Method section of the template, select "HTTP" and accept all defaults.

Health Monitor	
Name: *	wshc
Retry:	3
Consec Pass Req'd:	1
Interval:	5 Seconds
Timeout:	5 Seconds
Strictly Retry:	<input type="checkbox"/>
Disable After Down:	<input type="checkbox"/>
Method	
Override IPv4:	
Override IPv6:	
Override Port:	
Method:	<input checked="" type="radio"/> Internal <input type="radio"/> External
Type:	HTTP
Port:	80
Host:	
URL:	GET /
User:	
Password:	
Expect:	<input type="checkbox"/> Text <input type="checkbox"/> Code
Maintenance Code:	
<input checked="" type="button" value="OK"/> <input type="button" value="Cancel"/>	

Figure 17: Health Monitoring template

5. Click **OK**, then click **Save** to save the configuration.

The following figures show the HTTP health monitor selected on the Server and Service Group configuration pages.

General	
Name: *	wsph1
IP Address/Host: *	192.168.10.3
GSLB External IP Address:	
Weight:	1
Health Monitor:	wshc
Status:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Connection Limit:	8000000 <input checked="" type="checkbox"/> Logging

Figure 18: Health Monitor option on server



Service Group	
Name: *	SGWS
Type:	TCP
Algorithm:	Round Robin
Health Monitor:	wshc
Min Active Members:	<input type="checkbox"/>

Figure 19: Health Monitoring option on service group

Once the Health Monitor templates are applied, you can verify health status by viewing the server and service group lists pages in the GUI.

<input type="checkbox"/>	Name	IP Address/Host	Health Monitor	Status	Health
<input type="checkbox"/>	wsph1	192.168.10.3	wshc	✓	↑
<input type="checkbox"/>	wsph2	192.168.10.4	wshc	✓	↑
Select All Unselect All				Selected:	0

Figure 20: WebSphere Health Monitor

The status should look like this:  . If the status is down, this is how the health monitor should look like.  . Please verify that the IBM WebSphere servers are in service before moving forward with the deployment guide.

15 OPTIONAL: IBM WEBSHERE SIMPLE URL REDIRECT

The AX Series supports custom scripting with the aFlex scripting language. The aFlex scripting language can perform inline custom scripting for in-depth, granular control of inspection and redirection policies such as redirect, filter, drop and others. The aFlex scripting language is based on an industry standard Tool Command Language (TCL) scripting language. If you are interested in other aFlex scripts, please refer to:

http://www.a10networks.com/products/axseries-aflex_advanced_scripting.php

The purpose of the simple URL redirect is to redirect all traffic requests to a specific URL string. In addition, URL redirection offers URL shortening, which prevents broken links when a web page is moved, and minimizes client address (URL) confusion.

Sample URL Redirect:

```
when HTTP_REQUEST {
    if { [HTTP::uri] equals "/A10" } {
        HTTP::redirect http://\[HTTP::host\]/oss/signup.php
    }
}
```

```

    }
}

```

Note: The simple URL redirect script above is only a sample. The redirect URL address may vary depending on how the directory structure of a web site is provisioned within an IBM WebSphere application.

To add the script show above to the AX configuration:

1. Navigate to **Config Mode > Service > aFlex**.
2. Select **Add**.
3. Enter a name for the script: "SimpleRedirect"
4. Enter the script definition in the **Definition** field.
5. Click **OK**, then click **Save** to save the configuration.

The screenshot shows the 'aFlex' configuration window. The 'Name' field is set to 'SimpleRedirect'. The 'Definition' field contains the following script code:

```

when HTTP_REQUEST {
  if { [HTTP::uri] equals "/A10" } {
    HTTP::redirect http://[HTTP::host]/oss/signup.php
  }
}

```

Figure 21: aFlex Redirect Script

Note: Once the aFlex script is entered, bind the script to the virtual services port.

16 PREPARING THE CONFIGURATION

To configure the advanced WebSphere configuration, a few changes to the basic configuration are required:

- On the virtual server, add a new service type, "HTTPS".

- Import existing WebSphere web server SSL certificates signed by a certificate authority (CA), or create a self-signed on the AX.
- Create a client-SSL template.

16.1 ADD A NEW SERVICE TYPE HTTPS

Navigate to **Config Mode > Service > SLB > Virtual Service**.

1. Click **Add** within the port section.
2. From the Type drop-down menu, select “**HTTPS**”.
3. From the Service Group drop-down menu, select “**SGWS**”.

Virtual Server Port	
Virtual Server:	wsphvip
Type:	HTTPS
Port:	9443
Service Group:	SGWS

Figure 22: Virtual Server Port

Click **OK** and then click **Save** to store your configuration changes.

16.2 IMPORT SSL CERT OR CREATE SELF-SIGNED CA

There are two options to configure when installing an SSL template from the AX Series:

Option 1: Generate a Self-Signed CA from the AX: Self-signed CA is generated from the AX Series.

Option 2: Import an SSL Certificate and Key: Export existing CA certificate from WebSphere web servers and import to AX Series device.

16.2.1 OPTION 1: GENERATE A SELF-SIGNED CERTIFICATE

1. Navigate to **Config Mode > Service > SSL Management > Certificate**.
2. Click **Create**.
3. Enter the **File Name** of the certificate, “wpsh”.

4. From the Issuer drop-down list, select “Self”.
5. Enter the following values:
 - ◆ **Common Name:** “example.com”
 - ◆ **Division:** “example.com”
 - ◆ **Organization:** “example”
 - ◆ **Locality:** “SanJose”
 - ◆ **State or Province:** “CA”
 - ◆ **Country:** “USA”
 - ◆ **Email Address:** “admin@example.com”
 - ◆ **Valid Days:** “730” (Default)
 - ◆ **Key Size (Bits):** “2048”

Note: The AX Series can support 512-bit, 1028-bit, 2048-bit, and 4096-bit keys. The higher the bit size, the more CPU processing that will be required on the AX device.

General	
File Name:	lwsph

Certificate	
Issuer:	Self
Common Name:	example.com
Division:	example.com
Organization:	example
Locality:	SanJose
State or Province:	CA
Country (C):	United States of America US
Email Address:	admin@example.com
Valid Days:	730 days

Key	
Key Size:	2048 Bits

Figure 23: Self-Signed Certificate

6. Click **OK**, then click **Save** to save your configuration changes.

16.2.2 OPTION 2: IMPORT THE CERTIFICATE AND KEY

Before beginning this procedure, export your certificate and key from your IBM WebSphere server onto your PC.

1. Navigate to **Config Mode > SSL Management > Certificate**.
2. Click **Import** to add a new SSL certificate.
3. Enter a name for the certificate: "wsi".
4. Select **Local** or **Remote**, depending on the file location
5. Enter the **Certificate Password** (if applicable).
6. Click **Browse** and navigate to the certificate file.

Import	
Name: *	wsi
Import Certificate from:	<input checked="" type="radio"/> Local <input type="radio"/> Remote <input type="radio"/> Text
Certificate Format:	PEX
Password:	*****
Certificate Source:	C:\Temp\wsi.pfx <input type="button" value="Browse..."/>

Figure 24: Import Certificate

Note: If you are importing a CA-signed certificate for which you used the AX device to generate the CSR, you do not need to import the key. The key is automatically generated on the AX device when you generate the CSR.

7. Click **OK** and then click **Save** to store your configuration changes.

16.3 CREATE CLIENT-SSL TEMPLATE AND ENABLE SSL OFFLOAD

This section describes how to configure a client SSL template and apply it to the VIP.

1. Navigate to **Config Mode > Service > Template > SSL > Client SSL**.
2. Click **Add**.
3. Enter the **Name**: "wsphssl".
4. Enter the **Certificate Name**: "wsph".

5. Enter the **Key Name**: "wsph".
6. Enter the **Pass Phrase** (if applicable).

Client SSL	
Name:	wspncssl
Certificate Name:	wsph
Chain Cert Name:	
Key Name:	wsph
Pass Phrase:	
Confirm Pass Phrase:	
Cache Size:	0
SSL False Start:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled

Figure 25: Enabling SSL Offload

With SSL Offload configuration, the AX offloads the processing of SSL traffic from the WebSphere servers.

Once the client-SSL template is completed, you must bind it to the HTTPS virtual service (port 443), as follows:

1. Navigate to **Config Mode > Service > SLB > Virtual Server**.
2. Click on the Virtual Server name.
3. Select "9443" and click **Edit**.

Port						
<input type="checkbox"/>	Status	Port	Type	Service Group	<input type="button" value="Add"/>	<input type="button" value="Edit"/>
<input checked="" type="checkbox"/>	✓	9443	HTTPS	SGWSSSL	<input type="button" value="Delete"/>	<input type="button" value="Edit"/>
<input type="checkbox"/>	✓	9080	HTTP	SGWS	<input type="button" value="Enable"/>	<input type="button" value="Disable"/>

Figure 26: Virtual Server Port

4. Apply the Client SSL template by selecting it from the Client-SSL Template drop-down list.

Client-SSL Template:	wspncssl
----------------------	----------

Figure 27: Client-SSL template applied to virtual port

Click **OK** and then click **Save** to store your configuration changes.

17 HTTP/HTTPS COMPRESSION

HTTP/HTTPS Compression is a bandwidth optimization feature that compresses the HTTP objects requested from a web server. If your web site uses lots of bandwidth, enabling HTTP Compression will provide faster transmission times between a client's browser and web servers. The purpose of compression is to transmit the requested data more efficiently and with faster response times to the client. HTTP Compression makes HTTP requests much faster by transmitting less data.

17.1 CREATE HTTP COMPRESSION TEMPLATE

1. Navigate to **Config Mode > Service > Template > Application > HTTP**.
2. Click **Add**.
3. Enter a **Name**, "HTTP Compression".
4. Click **Compression** to display the compression configuration options.

Note: Compression is disabled by default. When compression is enabled, the compression options will have the default values shown in following example:

HTTP	
Name: *	HTTPCompression
Failover URL:	
Strict Transaction Switching:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Client IP Header Insert:	<input type="checkbox"/>
Retry HTTP Request:	<input type="checkbox"/>
<input type="checkbox"/>	Terminate HTTP 1.1 client when request has Connecton: close

Figure 28: HTTP Compression template

5. Select **Enabled** next to **Compression**.

Note: The AX Series offers various compression levels, ranging from levels 1 to 9. Level 1 is the recommended compression setting.

The screenshot shows the 'Compression' configuration column. The 'Compression' radio button is selected for 'Enabled'. The 'Keep Accept Encoding' radio button is selected for 'Disabled'. The 'Level' dropdown is set to '1 (least compression, fastest)'. The 'Min Content Length' is set to 120. There are three sections for 'Content Type', 'Exclude Content Type', and 'Exclude URI', each with an 'Add' and 'Delete' button.

Figure 29: Compression configuration column

6. Click **OK**, then click **Save** to save the configuration.

18 PERSISTENCE

There are multiple ways to apply persistence within the AX Series. The AX Series can offer Destination IP Persistence, Source IP Persistence, Cookie Persistence or SSL Session ID Persistence. The application that you will deploy on the IBM WebSphere dictates the persistence option required for a successful and functional deployment. For the details of the different persistence options of the AX Series, refer to the *AX Series-System and Administration Guide from the A10 Networks Support website*:

<http://www.a10networks.com/support-axseries/techlibrary.php>

In this example, the IBM WebSphere Application Servers will use the Cookie Persistence feature. Creation of the cookie persistence template is described below.

To enable cookie persistence, the template must be created first, as follows:

1. Navigate to **Config Mode > Service > Template > Cookie Persistence**.
2. Click **Add** to add a new cookie persistence template.
3. Enter the **Name**, "wsphcookie".
4. Select the **Expiration** radio button and enter "86400" in the **Seconds** field.

Cookie Persistence	
Name: *	wsphcookie
Expiration:	<input checked="" type="checkbox"/> 86400 Seconds
Cookie Name:	
Domain:	
Path:	
Match Type:	<input type="checkbox"/> Service Group <input type="text" value="Port"/>
Insert Always:	<input type="checkbox"/>
Don't Honor Conn Rules:	<input type="checkbox"/>

Figure 30: Cookie Persistence template

5. Click **OK**, then click **Save** to save the configuration.

Note: The different options available in persistence feature should be discussed with the IBM WebSphere software developer as every application has its own specific requirements.

19 CONNECTION REUSE

This section describes the AX Connection Reuse feature and how to configure it. Connection Reuse reduces the overhead associated with TCP connection setup, by establishing TCP connections with WebSphere Application Servers and then reusing those connections for multiple client requests. Connection Reuse significantly increases the responsiveness of the WebSphere Application Servers. This results in better WebSphere server performance and in improved scalability for production infrastructures.

1. Navigate to **Config Mode > > Service > Template > Connection Reuse**.
2. Click **Add**.
3. Enter the **Name**: "wsphcr".

Connection Reuse		
Name: *	wsphcr	
Limit Per Server:	1000	
Timeout:	2400	Seconds
Keep Alive Connections:	<input type="checkbox"/>	

Figure 31: Connection Reuse template

- Click **OK**, then click **Save** to save the configuration.

Note: The different options available in each acceleration feature should be discussed with the IBM WebSphere software developer, as every application has its own specific requirements.

20 RAM CACHING

RAM Caching allows cacheable data to be cached within the AX Series device itself, thus reducing overhead on the WebSphere web servers and increasing their capacity. RAM Caching reduces the number of connections and server requests that need to be processed.

- Navigate to **Config Mode > Service > Template > Application > RAM Caching**.
- Click **Add**.
- Enter or select the following values:
 - Name:** "wsphcr"
 - Age:** 3600 seconds
 - Max Cache Size:** 80 MB
 - Min Content Size:** 512 Bytes
 - Max Content Size:** 81920 Bytes
 - Replacement Policy:** "Least Frequently Used"

Note: The RAM Caching policy option is not required unless you have specific data that requires caching, no caching, or invalidation. These policy options can be configured in the Policy section of the RAM Caching template. For additional information on RAM caching policies, please refer to the AX Series Application Delivery and Server Load Balancing Guide.

RAM Caching		
Name:	wsphrc	
Age:	3600	Seconds
Max Cache Size:	80	MB
Min Content Size:	512	Bytes
Max Content Size:	81920	Bytes
Replacement Policy:	Least Frequently Used	
Accept Reload Request:	<input type="checkbox"/>	
Verify Host:	<input type="checkbox"/>	
Default Policy Ho-Cache:	<input type="checkbox"/>	
Insert Age:	<input checked="" type="checkbox"/>	
Insert Via:	<input checked="" type="checkbox"/>	

Figure 32: RAM Caching template

4. Click **OK**, then click **Save** to save the configuration.

21 APPLY OPTIMIZATION AND ACCELERATION FEATURE TEMPLATES ON VIP

After configuring the optimization and acceleration features, you must bind them to the virtual port on the VIP to place them into effect.

1. Navigate to **Config Mode > Service > SLB > Virtual Service**.
2. Click on the virtual service name.
3. Apply the features by selecting the templates from the applicable drop-down lists.

Source NAT Pool:	wssnat	
aFlx:	9080_9443	<input type="checkbox"/> Multiple
HTTP Template:	HTTPCompression	
RAM Caching Template:	wsphrc	
Client-SSL Template:	wsphcssl	
Server-SSL Template:		
Connection Reuse Template:	wsphcr	
TCP-Proxy Template:		
Persistence Template Type:	Cookie Persistence Template	
Cookie Persistence Template:	wsphcookie	
PBSLB Policy Template:		

Figure 33: Applying features

4. Click **OK**, then click **Save** to save the configuration.

22 SUMMARY AND CONCLUSION

The sections above show how to deploy the AX device for optimization of IBM WebSphere web servers. By using the AX device to load balance a pool of IBM WebSphere Application servers, the following key advantages are achieved:

- High availability for IBM WebSphere web servers to prevent web site failure, with no adverse impact on user access to applications
- Seamless distribution of client traffic across multiple IBM WebSphere web servers for site scalability
- Higher connection counts, faster end user responsiveness, and reduced IBM WebSphere web server CPU utilization by initiating SSL Offload, HTTP Compression, RAM Caching and Connection Reuse
- Improved site performance and reliability to end users

By using the AX Series Advanced Traffic Manager, significant benefits are achieved for all WebSphere web application users. For more information about AX Series products, please refer to the following URLs:

<http://www.a10networks.com/products/axseries.php>

<http://www.a10networks.com/resources/solutionsheets.php>

<http://www.a10networks.com/resources/casestudies.php>

A. CLI COMMANDS FOR SAMPLE BASIC CONFIGURATION

The following sections show the CLI commands for implementing the sample configurations described above.

```
hostname BasicAX

ip nat pool WSSNAT 192.168.10.225 192.168.10.225 netmask /24

health monitor wshc

    method tcp port 9080

slb server wsph1 192.168.10.3

    health-check ping

    port 9080 tcp
```

```
slb server wsph2 192.168.10.4
    health-check ping
    port 9080 tcp

slb service-group SGWS tcp
    health-check ping
    member wsph1:9080
    member wsph2:9080

slb template persist source-ip WSSIP
    match-type server

slb virtual-server wsphvip 192.168.10.200
    port 9080 http
    name _192.168.10.200_HTTP_9080
    source-nat pool WSSNAT
    service-group SGWS
    template persist source-ip WSSIP

end
```

B. CLI COMMANDS FOR SAMPLE ADVANCED CONFIGURATION

```
hostname AdvancedAX

ip nat pool WSSNAT 192.168.10.225 192.168.10.225 netmask /24

health monitor wshc
    method tcp port 9080

slb server wsph1 192.168.10.3
    health-check wshc
    port 9080 tcp
    port 9443 tcp
```

```
slb server wsph2 192.168.10.4
    health-check wshc
    port 9080 tcp
    port 9443 tcp

slb service-group SGWS tcp
    health-check wshc
    member wsph1:9080
    member wsph2:9080

slb service-group SGWSSSL tcp
    health-check wshc
    member wsph1:9443
    member wsph2:9443

slb template connection-reuse wsphcr

slb template cache wsphrc

slb template http HTTPCompression
    compression enable

slb template client-ssl wsphcssl
    cert wsph
    key wsph

slb template persist cookie wsphcookie
    expire 86400

slb template persist source-ip WSSIP
    match-type server

slb virtual-server wsphvip 192.168.10.200
    port 9080 http
    name _192.168.10.200_HTTP_9080
```

```
source-nat pool WSSNAT

service-group SGWS

port 9443 https

name _192.168.10.200_HTTPS_9443

source-nat pool WSSNAT

service-group SGWSSSL

template http HTTPCompression

template cache wphrc

template client-ssl wphcssl

template connection-reuse wphcr

template persist cookie wphcookie

end
```