Deployment Guide

AX Series for Oracle WebLogic 12*c*

TABLE OF CONTENTS

1 INTRODUCTION

A10 Networks and Oracle WebLogic provide a joint solution to deploy web and e-commerce applications. WebLogic Server is Java-based application server software that runs on a middle tier, between backend databases and related applications, and browser-based thin clients.

WebLogic is based on the Java 2 platform, Enterprise Edition (J2EE), the standard platform used to create Java-based multi-tier enterprise applications. WebLogic is the leading e-commerce online transaction processing (OLTP) platform. As the industry-leading OLTP, WebLogic Server allows you to quickly develop and deploy reliable, secure, scalable and manageable applications.

2 DEPLOYMENT GUIDE OVERVIEW

This deployment guide provides detailed instructions for deploying an A10 Networks AX Series Application Delivery Controller (ADC)/Server Load Balancer (SLB) with WebLogic Application Server (AS). The tested WebLogic solution has been installed on a multi-server installation of 64-bit Microsoft Windows 2008 Servers, with an A10 Networks AX Series deployed in front of the servers.

This deployment guide provides both basic and advanced configurations. The basic configuration provides load balancing of HTTP traffic. The advanced configurations provide the following enhancements:

- SSL Offload
- HTTP/HTTPS Compression
- Cookie Persistence
- Connection Reuse
- RAM Caching
- HTTP-to-HTTPS Redirect

The tested WebLogic application server is based on WebLogic version 12*c*.

3 DEPLOYMENT GUIDE PREREQUISITES

The testing of the solution in this deployment guide was based on the following requirements and lab setup:

- The A10 Networks AX Series device must be running AX Release 2.4.x or higher.

- The WebLogic 12*c* application server was tested and deployed on Windows 2008 (64-bit) Enterprise Edition Server Operating System.
- Java SE Development Kit (JDK) and Java Runtime Environment (JRE) are required on the application servers.

4 AX DEPLOYMENT FOR WEBLOGIC SERVER ROLES

WebLogic servers can be deployed to fulfill the following roles:

- **Application Servers** – Java-based pool of servers installed in the application server
- **Administration Server** – Configures and manages the application servers in a pool of servers. There are two options to manage WebLogic 12*c* application servers. You have the option to deploy a standalone management server or an Oracle Management Server.
- **Active Directory (AD) –** Deployment in which all Web Logic servers must be joined in a domain and in Active Directory Domain Services (ADDS).

5 ACCESSING THE AX SERIES ADC/SLB

This section describes how to log into 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)

Default Access Information:

- Default Username: “*admin”*
- Default password: “*a10*”

- Default IP Address of the device: “*172.31.31.31*”

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

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

6 ARCHITECTURE OVERVIEW

The diagram below shows the lab setup for Oracle WebLogic 12*c* with A10 Networks AX Series:

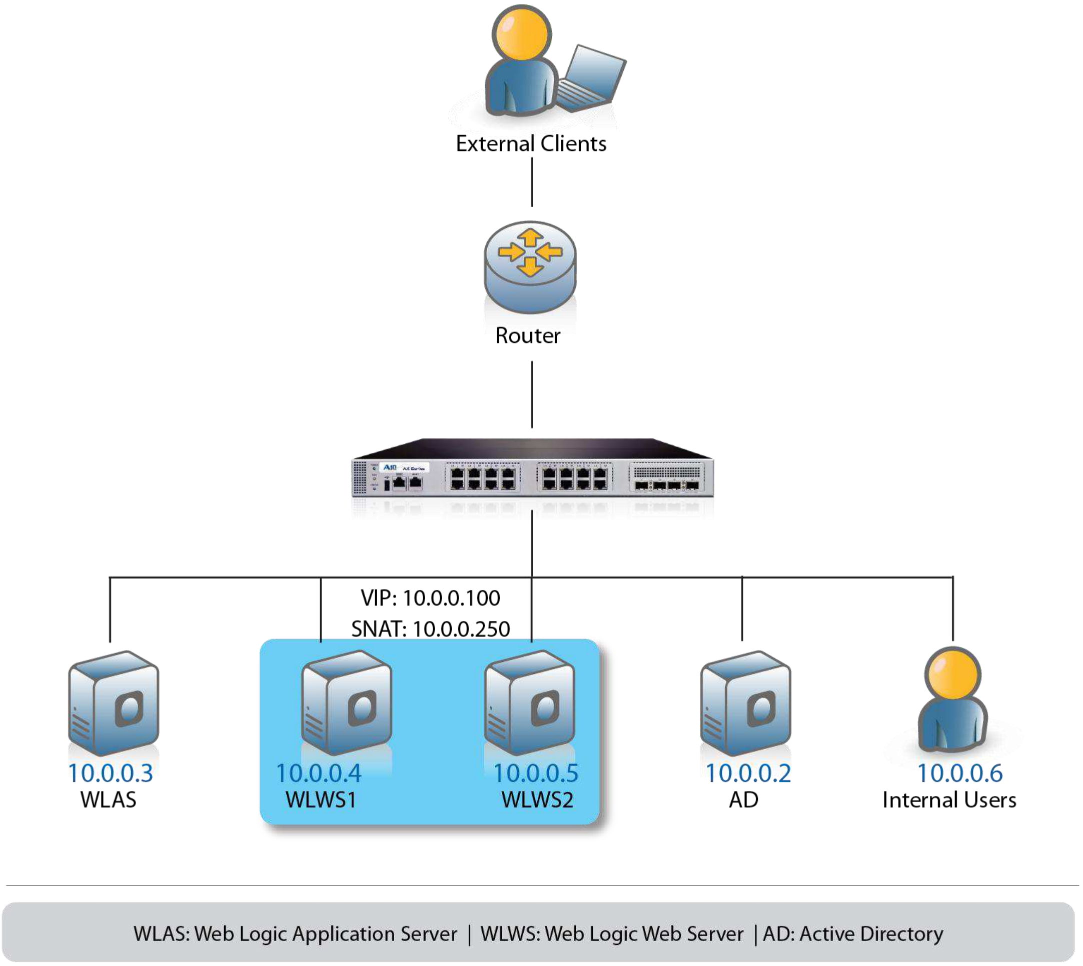


Figure 1: Oracle WebLogic 12c deployment topology

7 BASIC AX CONFIGURATION FOR WEBLOGIC

This section explains how the AX Series can be configured to load balance HTTP traffic. This section will provide detailed instructions for configuring real servers, a service group, virtual services, and virtual servers in a basic WebLogic implementation.

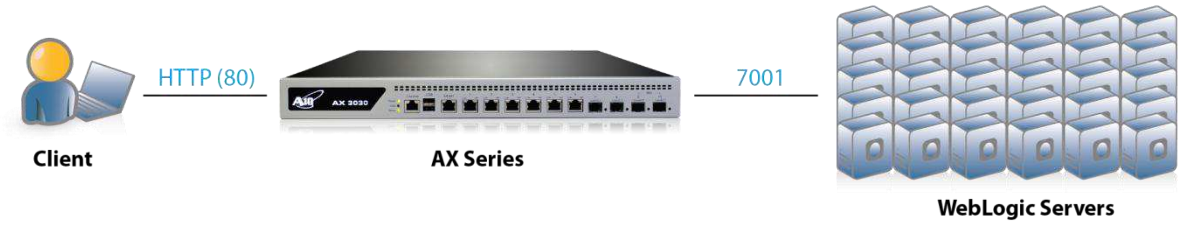


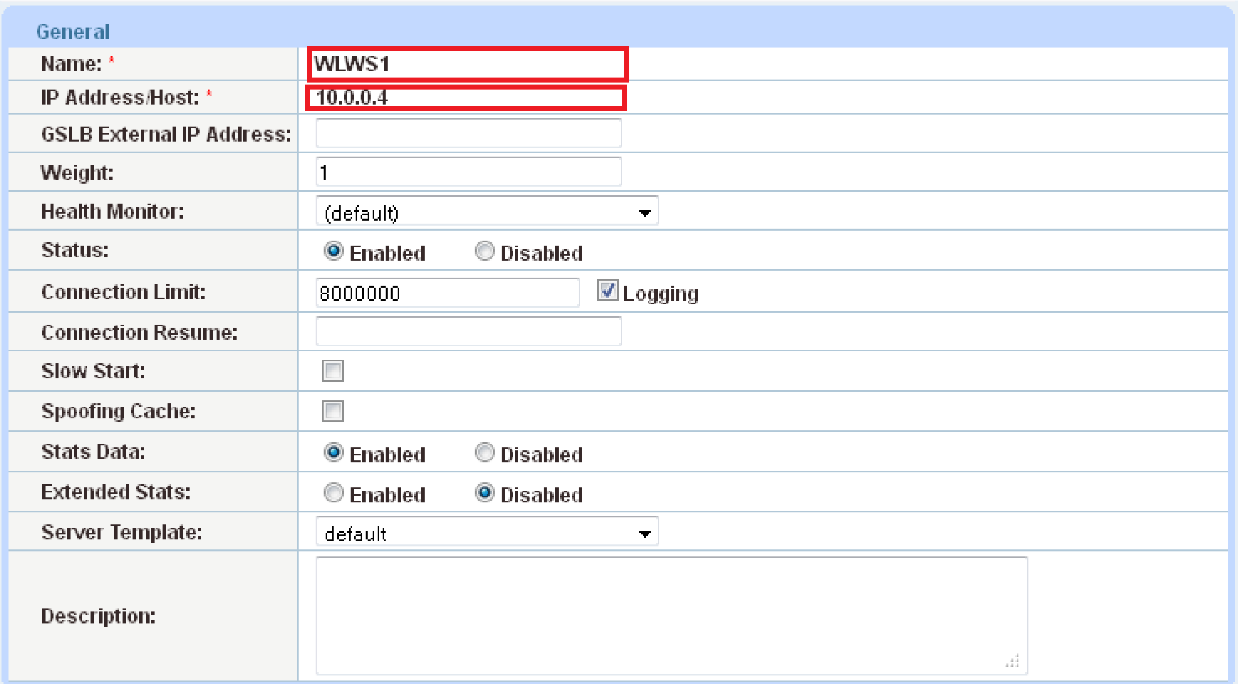
Figure 2: WebLogic HTTP configuration

7.1 SERVER CONFIGURATION

This section demonstrates how to configure the WebLogic servers in 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**: “WLWS1”
    - ♦ **IP address** /**Host**: *10.0.0.4*

Note: *Enter additional servers if necessary.*



General

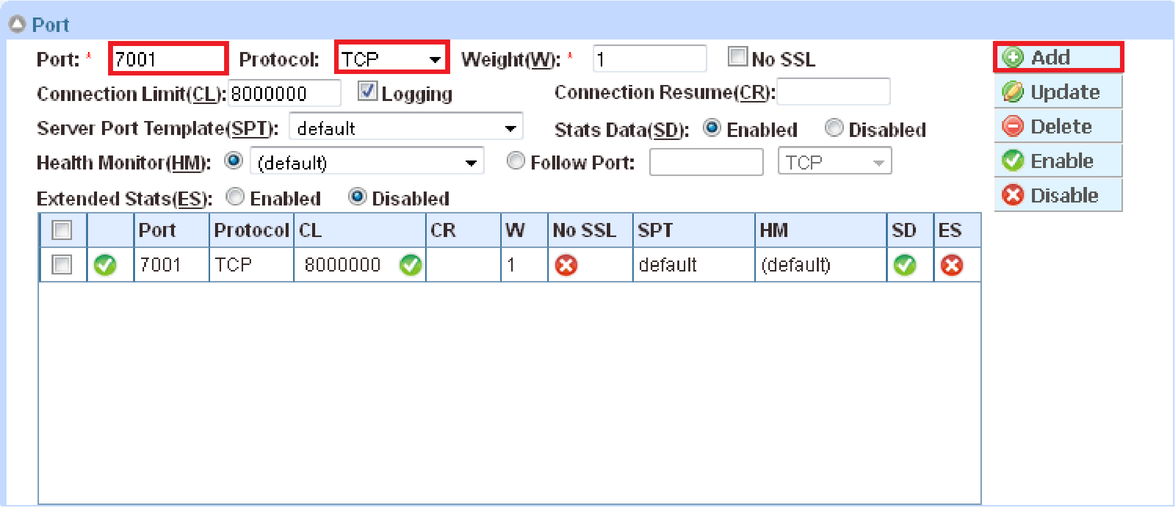
Name: *	WLWS1
IP Address/Host: *	10.0.0.4
GSLB External IP Address:	
Weight:	1
Health Monitor:	(default)
Status:	● Enabled ○ Disabled
Connection Limit:	8000000 ☑ Logging
Connection Resume:	
Slow Start:	□
Spoofing Cache:	□
Stats Data:	● Enabled ○ Disabled
Extended Stats:	○ Enabled ● Disabled
Server Template:	default
Description:	

Figure 3: Real server configuration

4. To add ports to the server configuration, enter the following information in the Port section:

    - **Port**: “7001”
    - **Protocol**: “TCP”

5. Click **Add**.



Port: * 7001 Protocol: TCP Weight(W): * 1 □ No SSL

Connection Limit(CL): 8000000 ☑ Logging Connection Resume(CR):

Server Port Template(SPT): default Stats Data(SD): ● Enabled ○ Disabled

Health Monitor(HM): ● (default) ○ Follow Port: TCP

Extended Stats(ES): ○ Enabled ● Disabled

□		Port	Protocol	CL	CR	W	No SSL	SPT	HM	SD	ES
□	✓	7001	TCP	8000000 ✓		1	☒	default	(default)	✓	☒

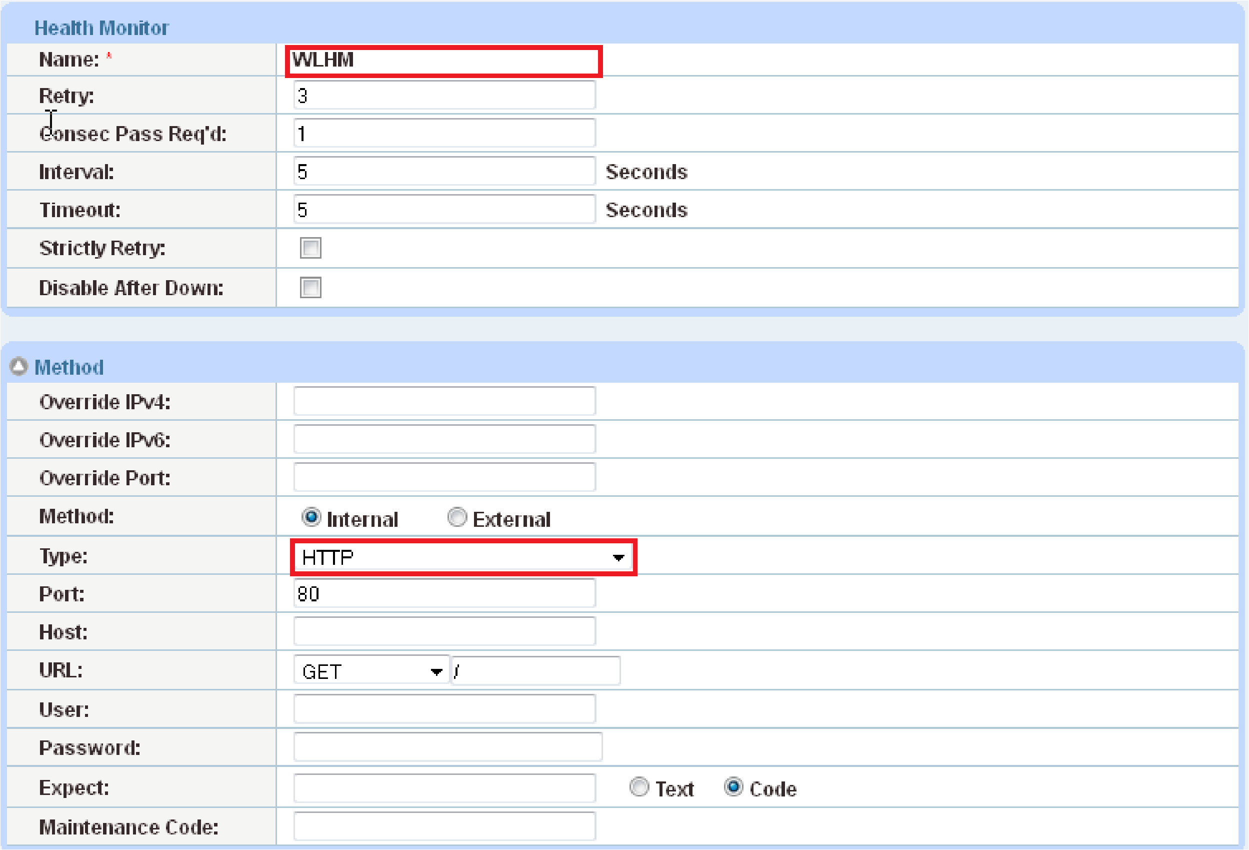
Figure 4: Real-server port configuration

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

7.2 HEALTH MONITOR CONFIGURATION

The AX series automatically can initiate the health status checks of real servers and service ports. This provides clients assurance 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 temporarily will be removed from the list of available servers. Once the server is restored and starts responding appropriately to the health checks, the server automatically will be added back to the list of available servers.

1. Navigate to **Config Mode** > **Service** > **Health Monitor**.
2. Click **Add** to add a health monitor.
3. Enter the Health Monitor **Name**, “WLHM”.
4. In the Method section, select **Type** “HTTP”.
5. Click **OK** and then continue by going to the Service Group configuration.



Health Monitor

Name: *	WLHM
Retry:	3
Consec Pass Req'd:	1
Interval:	5 Seconds
Timeout:	5 Seconds
Strictly Retry:	☐
Disable After Down:	☐

Method

Override IPv4:	
Override IPv6:	
Override Port:	
Method:	● Internal ○ External
Type:	HTTP
Port:	80
Host:	
URL:	GET /
User:	
Password:	
Expect:	○ Text ● Code
Maintenance Code:	

Figure 5: WebLogic health monitor configuration

7.3 SERVICE GROUP CONFIGURATION

This section demonstrates how to configure the WebLogic servers into a service group (pool). A service group contains a set of real servers from which the AX device can select to service client requests. A service group supports multiple WebLogic real servers accessed by clients as one logical server.

1. Navigate to **Config Mode** > **Service** > **SLB** > **Service Group**.

2. Click **Add** to add a new service group.

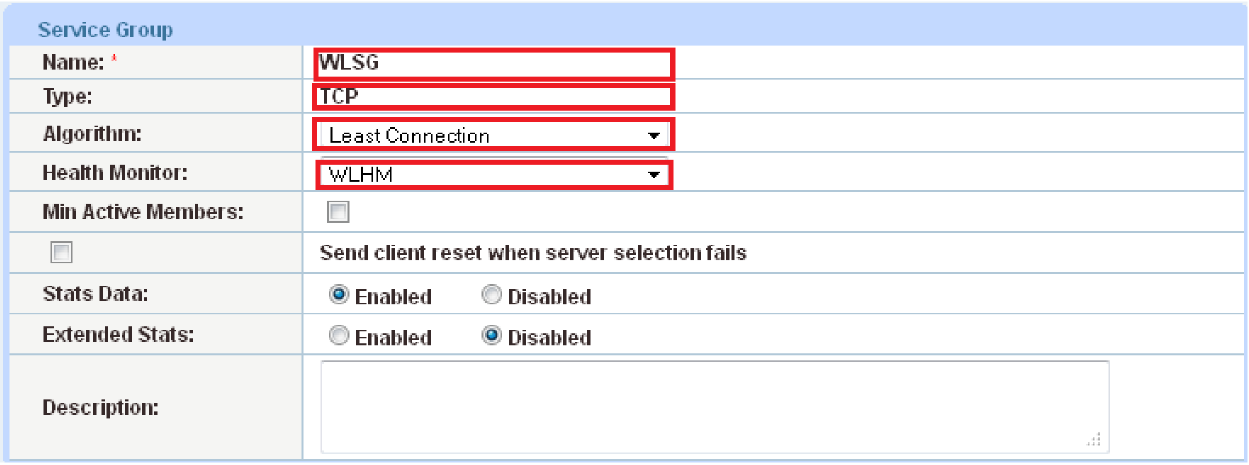
3. Within the Service Group section, enter the following required information:

   - **Name**: “WLSG”

   - **Type**: “TCP”

   - **Algorithm**: “Least Connection”

- **Health Monitor**: “WLHM”



Service Group

Name: *	WLSG
Type:	TCP
Algorithm:	Least Connection
Health Monitor:	WLHM
Min Active Members:	□
□	Send client reset when server selection fails
Stats Data:	● Enabled ○ Disabled
Extended Stats:	○ Enabled ● Disabled
Description:	

Figure 6: WebLogic service-group configuration

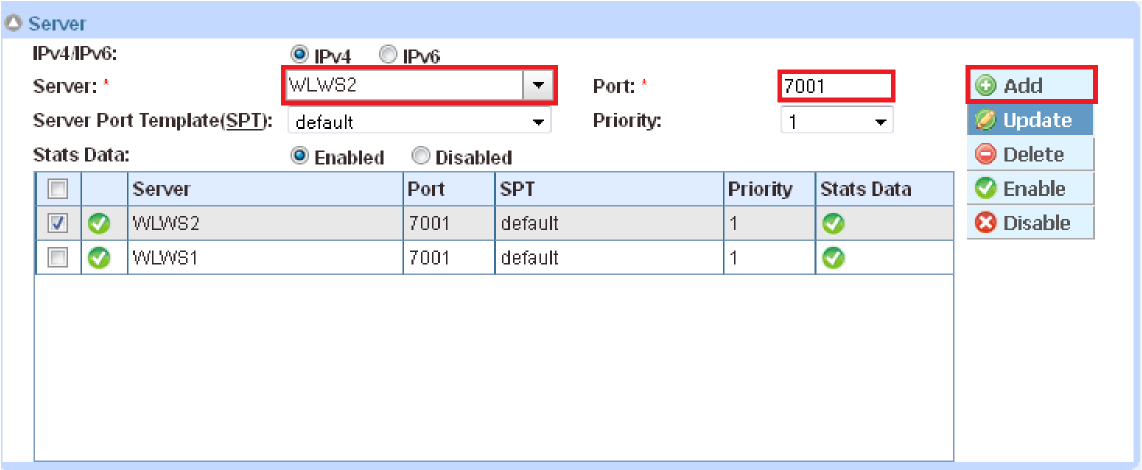
4. In the Server section, add one or more servers from the **Server** drop-down list:

   - **Server**: “WLWS1”

   - **Port**: “7001”

5. Click **Add** and repeat for each additional WebLogic server.

   In the following example, server names **WLWS1** and **WLWS2** are entered, each with port **7001**.



Server

IPv4/IPv6:	● IPv4 ○ IPv6		
Server: *	WLWS2	Port: *	7001
Server Port Template(SPT):	default	Priority:	1
Stats Data:	● Enabled ○ Disabled		

□		Server	Port	SPT	Priority	Stats Data
☑	✓	WLWS2	7001	default	1	✓
□	✓	WLWS1	7001	default	1	✓

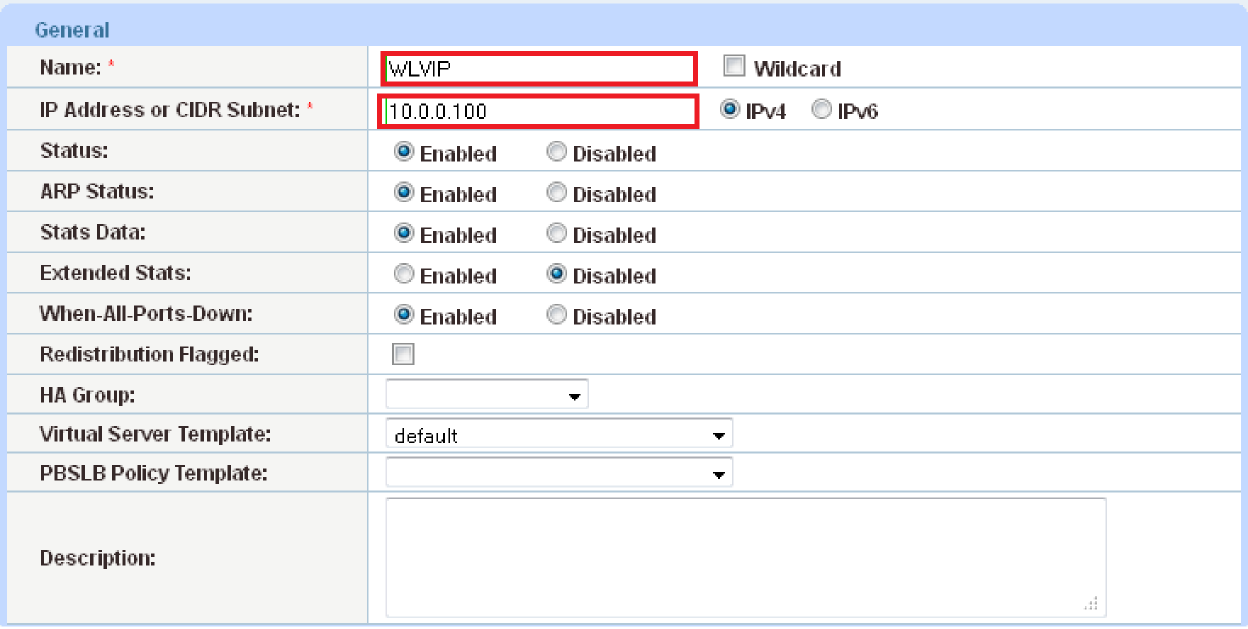
Figure 7: Service-group server configuration

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

7.4 VIRTUAL SERVER CONFIGURATION

This section demonstrates how to configure the virtual server (VIP) on the AX Series. Adding the virtual server ports within the AX Series will generate a virtual service list based on the protocol type selected.

1. Navigate to **Config Mode** > **Service** > **SLB** > **Virtual Server**.
2. Click **Add**.
3. Within the General section, enter the following required information:
   - ♦ **Name**: “WLVIP”
   - ♦ **IP Address or CIDR Subnet**: “*10.0.0.100”*



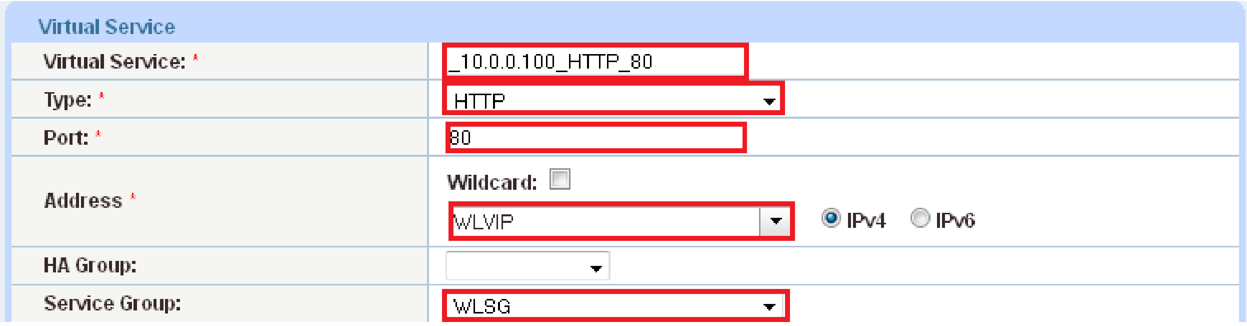
General

Name: *	WLVIP	□ Wildcard
IP Address or CIDR Subnet: *	10.0.0.100	● IPv4 ○ IPv6
Status:	● Enabled ○ Disabled	
ARP Status:	● Enabled ○ Disabled	
Stats Data:	● Enabled ○ Disabled	
Extended Stats:	○ Enabled ● Disabled	
When-All-Ports-Down:	● Enabled ○ Disabled	
Redistribution Flagged:	□	
HA Group:		
Virtual Server Template:	default	
PBSLB Policy Template:		
Description:		

Figure 8: WebLogic virtual server (VIP) configuration

4. In the Port section, click **Add**.
5. Enter the following Virtual Server Port information.
   - ♦ **Type**: “HTTP”

- **Port**: "80"
- **Address**: "WLVIP"
- **Service Group**: select: "WLSG" to bind the virtual server to the real servers.



Virtual Service

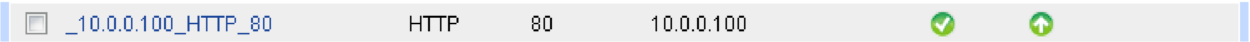
Virtual Service: *	_10.0.0.100_HTTP_80
Type: *	HTTP
Port: *	80
Address *	Wildcard: □ WLVIP ● IPv4 ○ IPv6
HA Group:	
Service Group:	WLSG

Figure 9: WebLogic virtual-server port configuration

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

7.4.1 ACCESSING VIRTUAL SERVICES (VIRTUAL PORTS) DIRECTLY

To view or modify virtual services without the need to navigate through the VIP configuration first, navigate to **Config Mode** > **Service** > **SLB** > **Virtual Service**. A list of the configured virtual services for all virtual servers is displayed.



□	_10.0.0.100_HTTP_80	HTTP	80	10.0.0.100	✓	↑

Figure 10: WebLogic virtual services list

7.5 IP SOURCE PERSISTENCE

The AX Series can support different modes of persistence, including the following:

- Cookie persistence
- Destination-IP persistence
- Source-IP persistence

- SSL-session-ID persistence

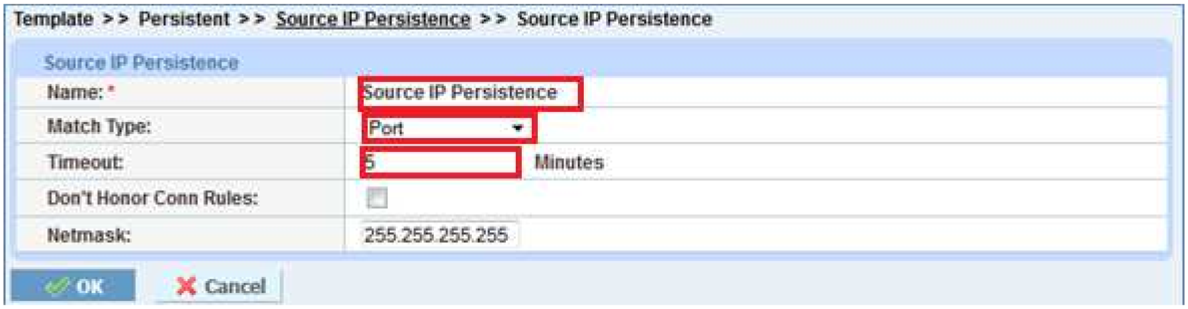
This deployment guide focuses on Source-IP persistence in the basic WebLogic configuration. Cookie persistence configuration will be featured within the Advanced WebLogic section.

7.5.1 CREATE IP PERSISTENCE TEMPLATE

1. Navigate to **Config Mode> Service** > **Template** > **Persistent** > **Source IP Persistence**.
2. Click **Add**.
3. Enter the following information:
   - **Name**: "Source IP Persistence"
   - **Match Type**: "Port"

Note: *Leave the* ***Timeout*** *set to its default (5 minutes).*

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



Template >> Persistent >> Source IP Persistence >> Source IP Persistence

Source IP Persistence

Name: *	Source IP Persistence
Match Type:	Port
Timeout:	5 Minutes
Don't Honor Conn Rules:	□
Netmask:	255.255.255.255

Figure 11: WebLogic Source-IP persistence template

7.5.2 APPLY IP PERSISTENCE TO THE VIP

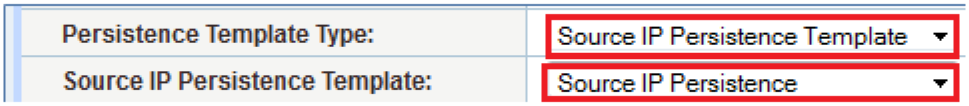
To assign the Source-IP persistence template to the VIP:

1. Navigate to **Config Mode> Service** > **SLB** > **Virtual Server**.
2. Click on the virtual server (VIP) name, "WLVIP".
3. In the Port section, select the checkbox next to the port in the port list, and click **Edit**.

4. From the **Persistence Template type** drop-down list, select "Source IP Persistence Template". This displays the **Source IP Persistence Template** drop-down list.

5. From the **Source IP Persistence Template** drop-down list, select the template.

The name "*Source IP Persistence*" is used as the template name in the example below.



Persistence Template Type:	Source IP Persistence Template
Source IP Persistence Template:	Source IP Persistence

Figure 12: Source-IP persistence assignment to the virtual port

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

7.6 IP SOURCE NAT

Since the lab setup was configured in "**one-arm**" mode, Source NAT (SNAT) is required. The SNAT template must be applied to the virtual server port for SNAT to take effect.

7.6.1 CREATE IP SOURCE NAT TEMPLATE

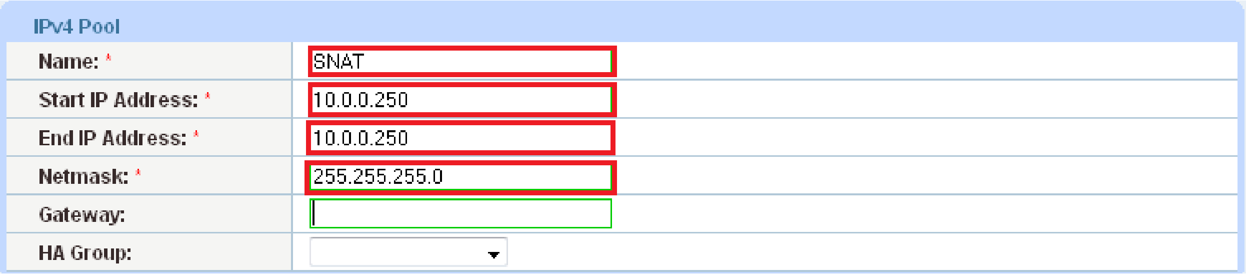
Note: *One SNAT IP address can be used for up to 64,000 flows. If the WebLogic environment will consist of many concurrent users, it is advisable to configure multiple SNAT IP addresses.*

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

2. Click **Add**.

3. Enter the following information:

   - **IP Source NAT Name**: "SNAT"
   - **Enter Start IP Address**:*10.0.0.250* (Example)
   - **Enter End IP Address**: *10.0.0.250* (Example)
   - **Enter Netmask**: *255.255.255.0*



IPv4 Pool

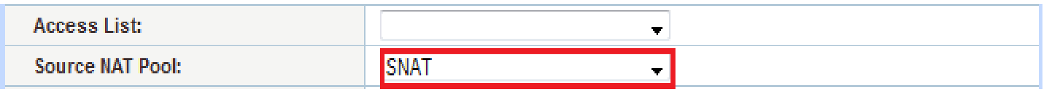
Name: *	SNAT
Start IP Address: *	10.0.0.250
End IP Address: *	10.0.0.250
Netmask: *	255.255.255.0
Gateway:	
HA Group:	

Figure 13: IP Source NAT configuration

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

7.6.2 APPLY IP SOURCE NAT TO THE VIP

1. Navigate to **Config Mode** > **Service** > **SLB** > **Virtual Server**.
2. Click on the virtual server (VIP) name, “WLVIP”.
3. In the Port section, select the checkbox next to the port in the port list, and click **Edit**.
4. From the **Source NAT Pool** drop-down list, select the pool configured in the previous section.



Access List:	
Source NAT Pool:	SNAT

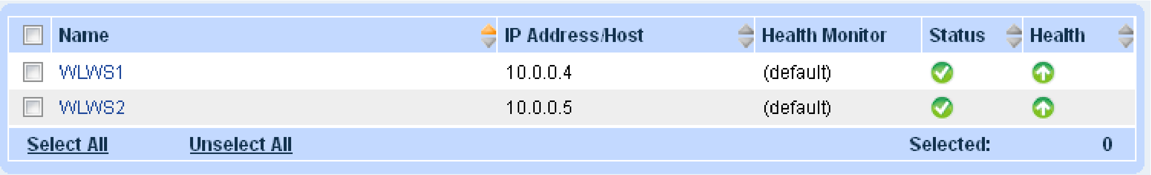
Figure 14: SNAT configuration

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

8 VALIDATE SERVICE

To validate that the basic configuration is functioning correctly:

1. Navigate to **Config Mode** > **Service** > **SLB** > **Server**.
2. Verify that the **Status** and **Health** states for the real server(s) are green: ⬆ ✓

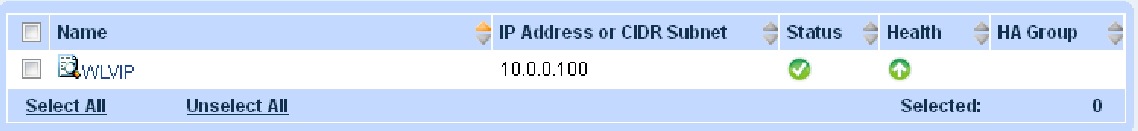


□	Name	IP Address/Host	Health Monitor	Status	Health
□	WLWS1	10.0.0.4	(default)	✓	↑
□	WLWS2	10.0.0.5	(default)	✓	↑

Figure 15: Health and status check for real servers

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

4. Verify that the **Status** and **Health** states for the virtual server are green: ↑ ✓

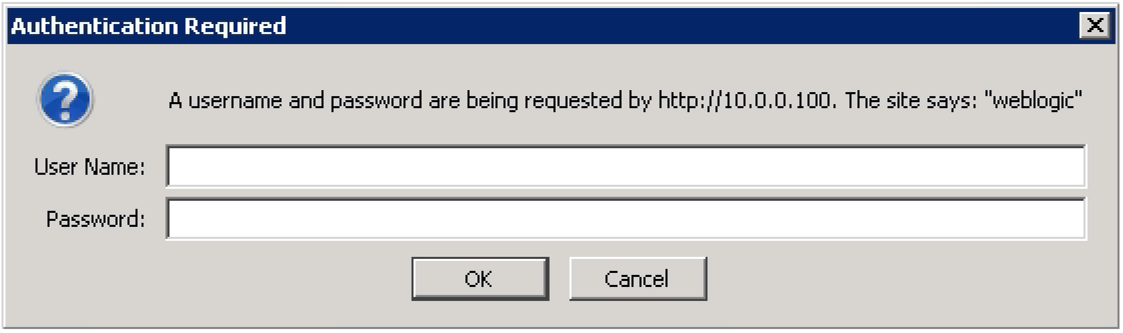


□	Name	IP Address or CIDR Subnet	Status	Health	HA Group
□	WLVIP	10.0.0.100	✓	↑	

Figure 16: Health and status check for real servers for VIP

5. Launch a web browser and navigate to the VIP address: (Example: *10.0.0.100* = www.example.com)

6. Enter the required **User Name** and **Password** for login.



Authentication Required

A username and password are being requested by http://10.0.0.100. The site says: "weblogic"

User Name:

Password:

Figure 17: WebLogic login

9 ADVANCED AX FEATURES FOR WEBLOGIC

This section describes advanced traffic optimization features that an administrator can add within the basic WebLogic configuration. These features provide web application acceleration and optimization of WebLogic servers. These features can be configured by creating templates and applying the templates to the virtual service.

WebLogic supports SSL, which is highly recommended when deploying in a production environment.

The URL address below provides information on configuring WebLogic to support SSL:

http://docs.oracle.com/cd/E13222_01/wls/docs90/secmanage/ssl.html

9.1 PREPARING THE CONFIGURATION

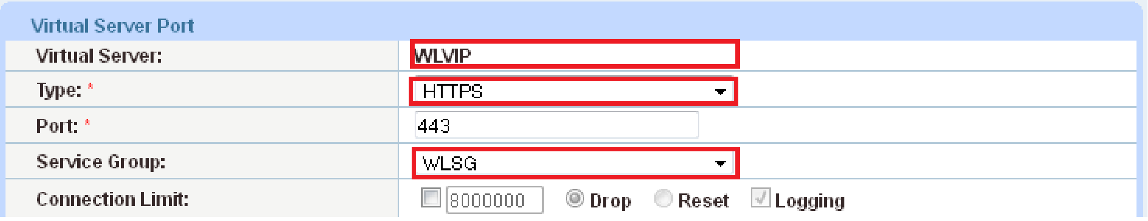
To configure the advanced WebLogic configuration, a few changes to the basic configuration are required:

- On the virtual server, add a new service type, “HTTPS”.
- Import existing WebLogic webserver SSL certificates signed by a certificate authority (CA),or create a self-signed on the AX.
- Create a client-SSL template.

9.2 ADD A NEW SERVICE TYPE HTTPS

1. Navigate to **Config Mode** > **Service** > **SLB** > **Virtual Service**.
2. Click **Add** within the port section.
3. From the Type drop-down menu, select “HTTPS”.
4. From the Service Group drop-down menu, select “WLSG”.

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



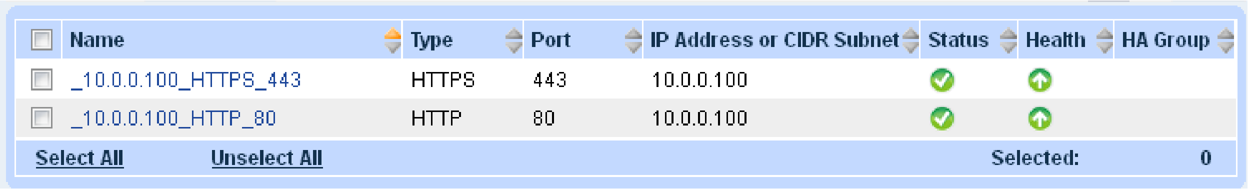
Virtual Server Port

Virtual Server:	WLVIP
Type: *	HTTPS
Port: *	443
Service Group:	WLSG
Connection Limit:	□ 8000000 ● Drop ○ Reset ☑ Logging

Figure 18: Virtual server port configuration

Configuration Check:

Once the new service type, HTTPS, is configured, navigate to **Config Mode** > **Service** > **SLB** > **Virtual Service**. This is how the configuration should look once the HTTPS Virtual Service has been added:



□	Name	Type	Port	IP Address or CIDR Subnet	Status	Health	HA Group
□	_10.0.0.100_HTTPS_443	HTTPS	443	10.0.0.100	✓	↑	
□	_10.0.0.100_HTTP_80	HTTP	80	10.0.0.100	✓	↑	

Figure 19: Configuration check

9.3 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 WebLogic webservers and import to AX Series device.

9.3.1 OPTION 1: GENERATE A SELF-SIGNED ON THE AX DEVICE

1. Navigate to **Config Mode** > **SSL Management** > **Certificate**.

2. Click **Create** to add a new SSL certificate.

3. Enter the **File Name** of the certificate: “WS”.

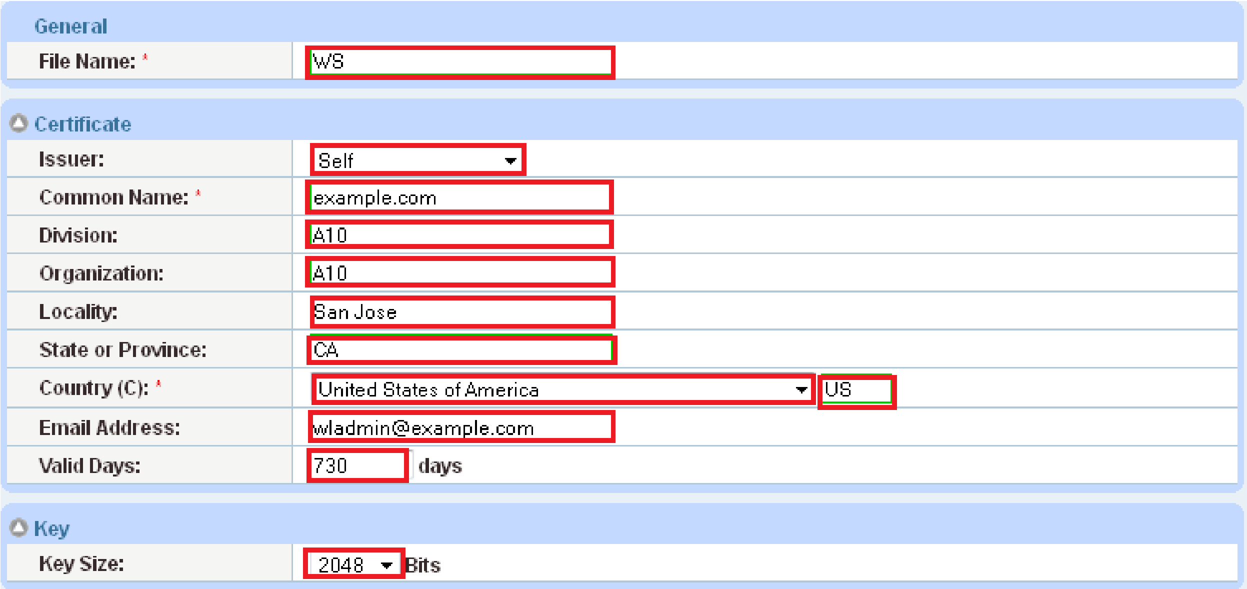
4. From the **Issuer** drop-down menu, select “Self”, and enter the following values:

- **Common Name**: “example.com”
- **Division**: “A10”
- **Organization**: “A10”
- **Locality**: San Jose
- **State or Province**: “CA”
- **Country**: “USA”
- **Email Address**: “wladmin@example.com”
- **Valid Days**: “730” (Default)

- **Key Size (Bits)**: “2048”

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

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



General

File Name: *	WS

Certificate

Issuer:	Self
Common Name: *	example.com
Division:	A10
Organization:	A10
Locality:	San Jose
State or Province:	CA
Country (C): *	United States of America US
Email Address:	wladmin@example.com
Valid Days:	730 days

Key

Key Size:	2048 Bits

Figure 20: Self-signed SSL certificate

9.3.2 OPTION 2: IMPORT CA-SIGNED SSL CERTIFICATE AND KEY

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

1. Navigate to **Config Mode** > **SSL Management** > **Certificate**.

2. Click **Import** to add a new SSL certificate.

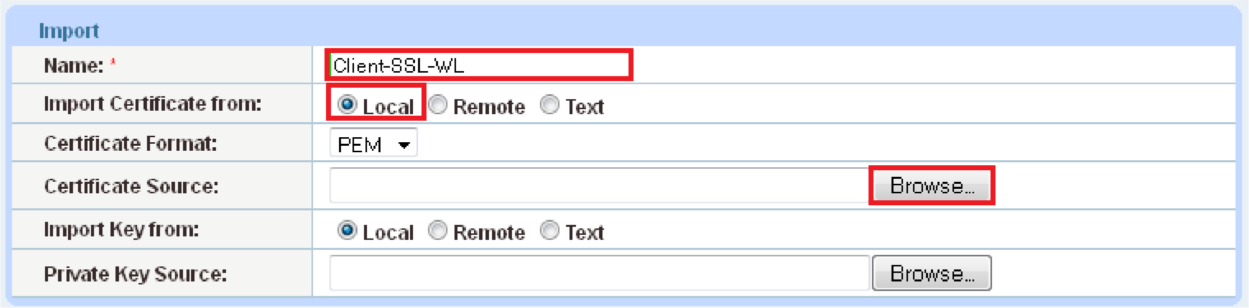
3. Enter a name for the certificate: “Client-SSL-WL”.

4. Select **Local** next to **Import Certificate from**.

Note: *Your selection depends on the location of the certificate. The AX Series can import certificates from local or remote storage, or from copy-and-pasted text.*

5. Click **Browse** and navigate to the certificate file.

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.*



Import

Name: *	Client-SSL-WL
Import Certificate from:	● Local ○ Remote ○ Text
Certificate Format:	PEM
Certificate Source:	Browse...
Import Key from:	● Local ○ Remote ○ Text
Private Key Source:	Browse...

Figure 21: Import SSL certificate

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

9.3.3 CREATE CLIENT-SSL TEMPLATE

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.

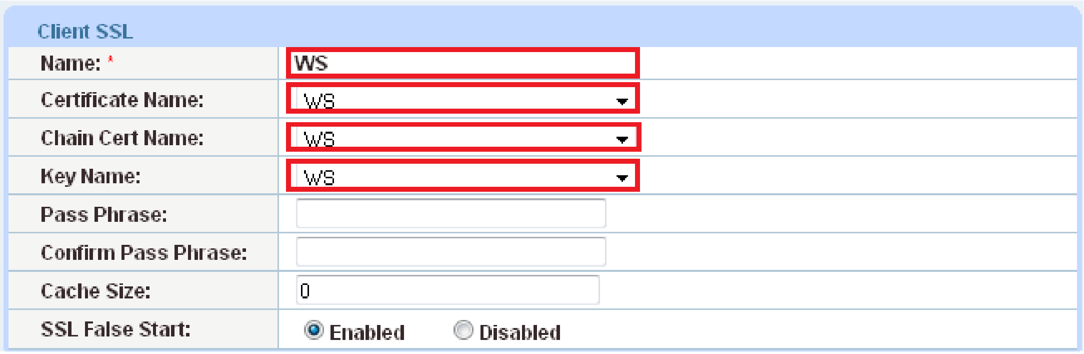
2. Click **Add**.

3. Enter the **Name**: “WS”.

4. Enter the **Certificate Name**: “WS”.

5. Enter the **Key Name**: “WS”.

6. Enter the **Pass Phrase** (if applicable)



Client SSL

Name: *	WS
Certificate Name:	WS
Chain Cert Name:	WS
Key Name:	WS
Pass Phrase:	
Confirm Pass Phrase:	
Cache Size:	0
SSL False Start:	● Enabled ○ Disabled

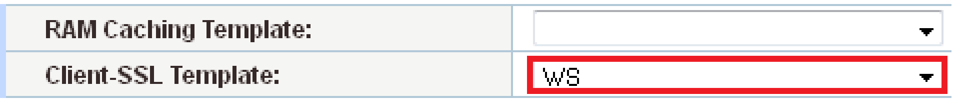
Figure 22: Client-SSL template

9.3.4 TO APPLY THE NEW CLIENT-SSL TEMPLATE AND ENABLE SSL OFFLOAD

With SSL Offload configuration, the AX offloads the processing of SSL traffic from the WebLogic 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 Serve**r name.
3. Select “443” and click **Edi**t.
4. Apply the Client SSL template by selecting it from the **Client-SSL Template** drop-down list.
5. Click **OK** and then click **Save** to store your configuration changes.



RAM Caching Template:	
Client-SSL Template:	WS

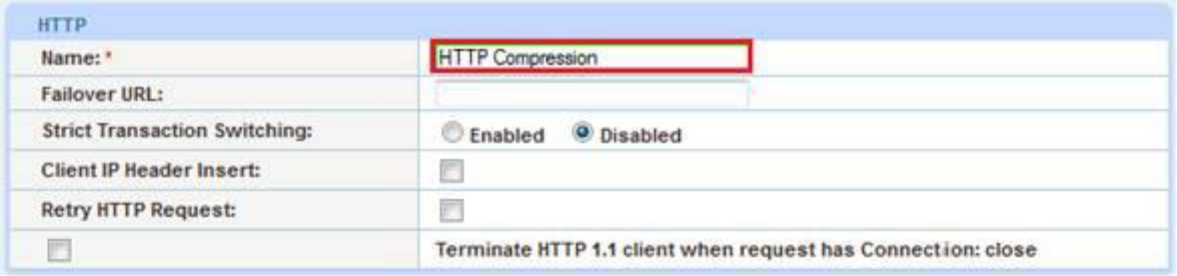
Figure 23: Client-SSL template applied to virtual port

9.4 HTTP/HTTPS COMPRESSION

To configure HTTP/HTTPS Compression, create an HTTP template with compression settings and apply the template to the virtual port.

9.4.1 CONFIGURE HTTP TEMPLATE

1. Navigate to **Config Mode** > **Template** > **Application** > **HTTP**.
2. Click **Add**.
3. Enter a **Name**: “HTTP Compression”.



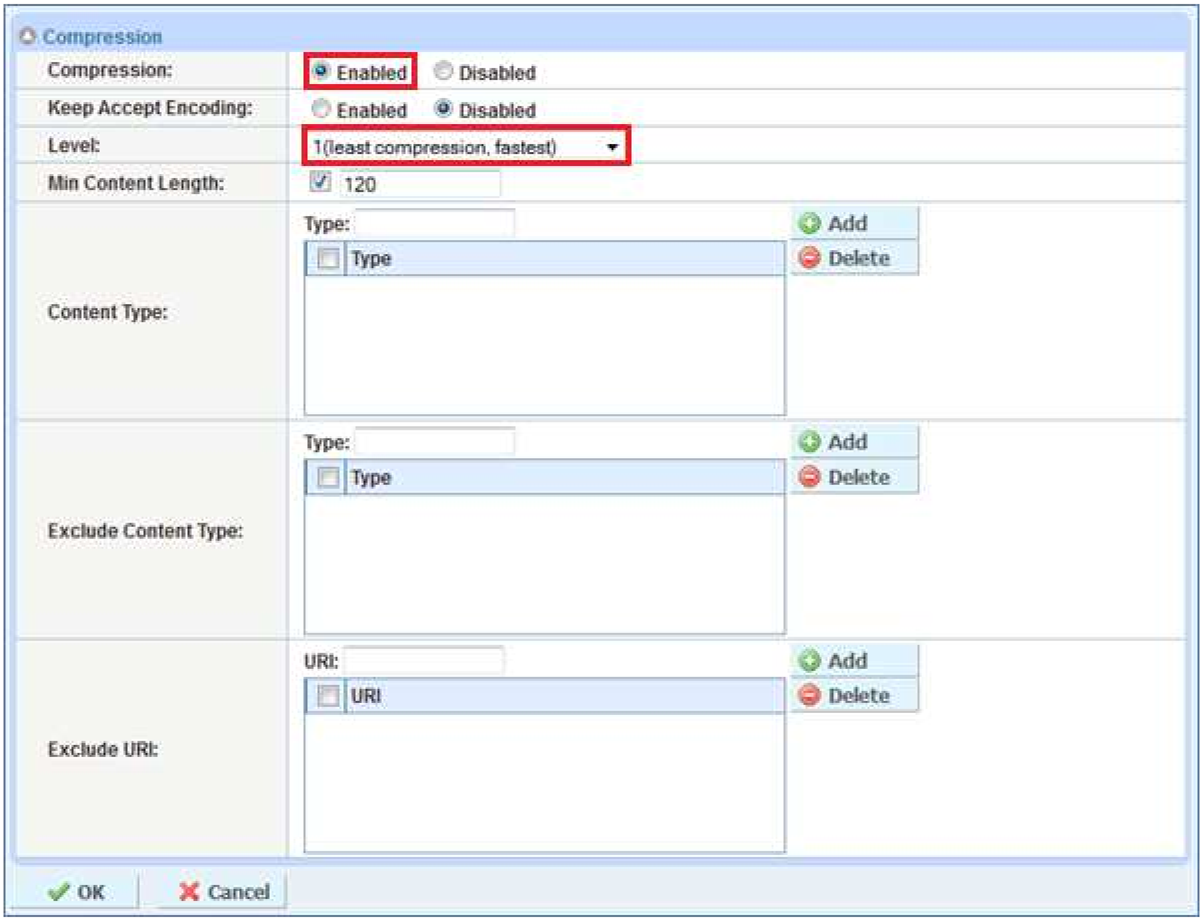
HTTP

Name: *	HTTP Compression
Failover URL:	
Strict Transaction Switching:	○ Enabled ● Disabled
Client IP Header Insert:	□
Retry HTTP Request:	□
□	Terminate HTTP 1.1 client when request has Connection: close

Figure 24: HTTP template with compression

4. Click **Compression** to display the compression configuration options.
5. Select **Enabled** next to **Compression**.

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



Compression

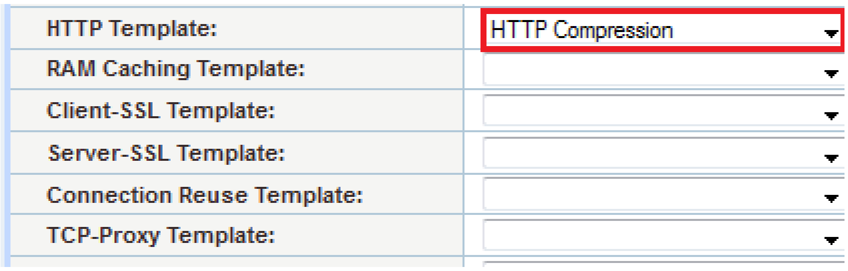
Compression:	● Enabled ○ Disabled
Keep Accept Encoding:	○ Enabled ● Disabled
Level:	1(least compression, fastest)
Min Content Length:	☑ 120
Content Type:	Type: □ Type
Exclude Content Type:	Type: □ Type
Exclude URI:	URI: □ URI

Figure 25: Compression configuration

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

9.4.2 APPLY HTTP TEMPLATE TO VIP

1. Navigate to **Config Mode** > **Service** > **SLB** > **Virtual Server**.
2. Click on the virtual server (VIP) name, “WLVIP”.
3. In the Port section, select the checkbox next to the port in the port list, and click **Edit**.
4. From the **HTTP Template** drop-down list, select the HTTP template configured in the previous section.



HTTP Template:	HTTP Compression
RAM Caching Template:	
Client-SSL Template:	
Server-SSL Template:	
Connection Reuse Template:	
TCP-Proxy Template:	

Figure 26: HTTP compression template applied to virtual port

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

9.5 COOKIE PERSISTENCE

To configure cookie persistence, create a cookie-persistence template and apply the template to the virtual port.

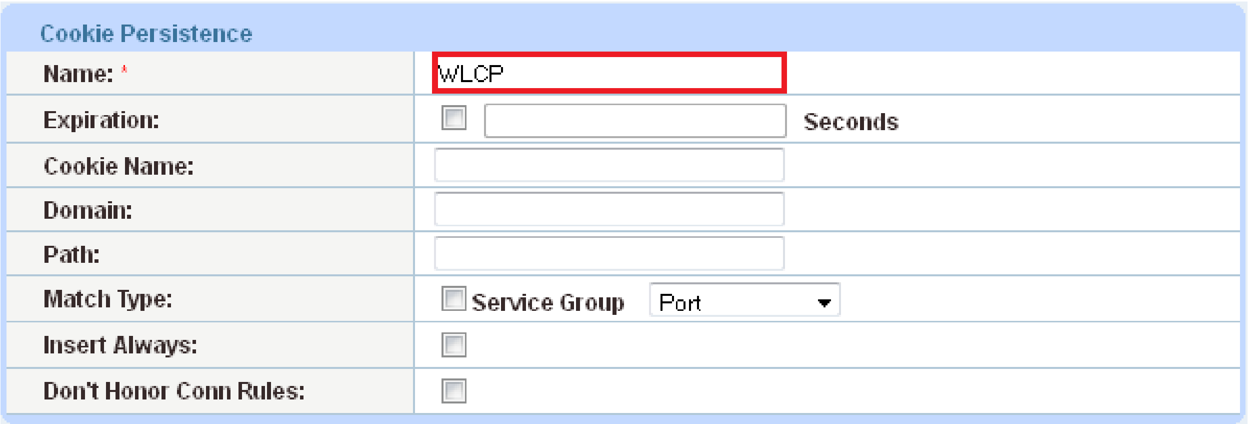
9.5.1 CONFIGURE COOKIE-PERSISTENCE TEMPLATE

1. Navigate to **Config Mode** > **Template** > **Persistent** > **Cookie Persistence**.

2. Click **Add**.

3. Enter the following information:

- **Name**: "WLCP"
- **Expiration**: select the checkbox and enter "86400" in the **Seconds** field.



Cookie Persistence

Name: *	WLCP
Expiration:	□ Seconds
Cookie Name:	
Domain:	
Path:	
Match Type:	□ Service Group Port
Insert Always:	□
Don't Honor Conn Rules:	□

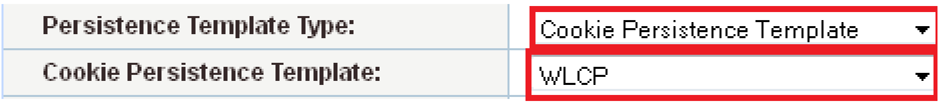
Figure 27: Cookie-persistence template

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

9.5.2 APPLY COOKIE-PERSISTENCE TEMPLATE TO VIP

1. Navigate to **Config Mode** > **Service** > **SLB** > **Virtual Server**.
2. Click on the virtual server (VIP) name, “WLVIP”.
3. In the Port section, select the checkbox next to the port in the port list, and click **Edit**.
4. From the **Persistence Template type** drop-down list, select “Cookie Persistence Template”. This displays the **Cookie Persistence Template** drop-down list.
5. From the **Cookie Persistence Template** drop-down list, select the template configured above.

The name “*WLCP*” is the template name in the example below.



Persistence Template Type: Cookie Persistence Template

Cookie Persistence Template: WLCP

Figure 28: Cookie-persistence template applied to virtual port

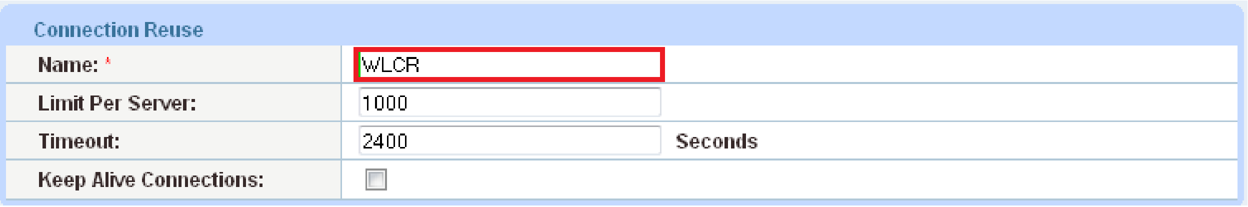
6. Click **OK**, then click **Save** to save the configuration.

9.6 CONNECTION REUSE (TCP OFFLOAD)

To configure Connection Reuse, create a connection-reuse template and apply the template to the virtual port.

9.6.1 CONFIGURE CONNECTION-REUSE TEMPLATE

1. Navigate to **Config Mode** > **Template** > **Connection Reuse**.
2. Click **Add**.
3. Enter the **Name**, “WLCR”.
4. Click **OK**, then click **Save** to save the configuration.



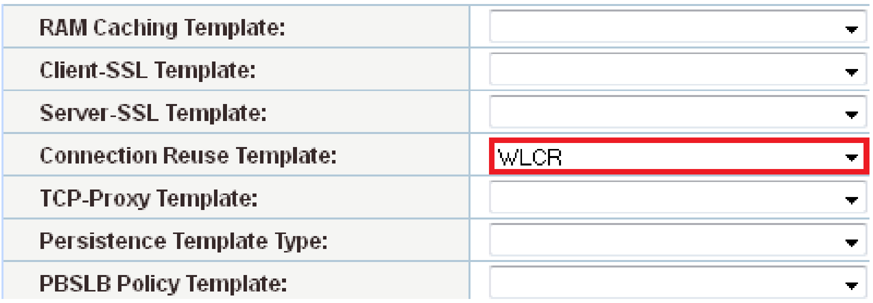
Connection Reuse

Name: *	WLCR
Limit Per Server:	1000
Timeout:	2400 Seconds
Keep Alive Connections:	□

Figure 29: Connection-reuse template

9.6.2 APPLY CONNECTION-REUSE TEMPLATE TO VIP

1. Navigate to **Config Mode** > **Service** > **SLB** > **Virtual Server**.
2. Click on the virtual server (VIP) name, “WLVIP”.
3. In the Port section, select the checkbox next to the port in the port list, and click **Edit**.
4. From the **Connection Reuse Template** drop-down list, select the template configured above.



RAM Caching Template:	
Client-SSL Template:	
Server-SSL Template:	
Connection Reuse Template:	WLCR
TCP-Proxy Template:	
Persistence Template Type:	
PBSLB Policy Template:	

Figure 30: Connection-reuse template applied to virtual port

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

9.7 RAM CACHING

To configure RAM Caching, create a RAM Caching template and apply the template to the virtual port.

9.7.1 CREATE RAM CACHING TEMPLATE

1. Navigate to **Config Mode** > **Template** > **Application** > **RAM Caching**.
2. Click **Add**.
3. Enter the **Name**: “WLRC”.

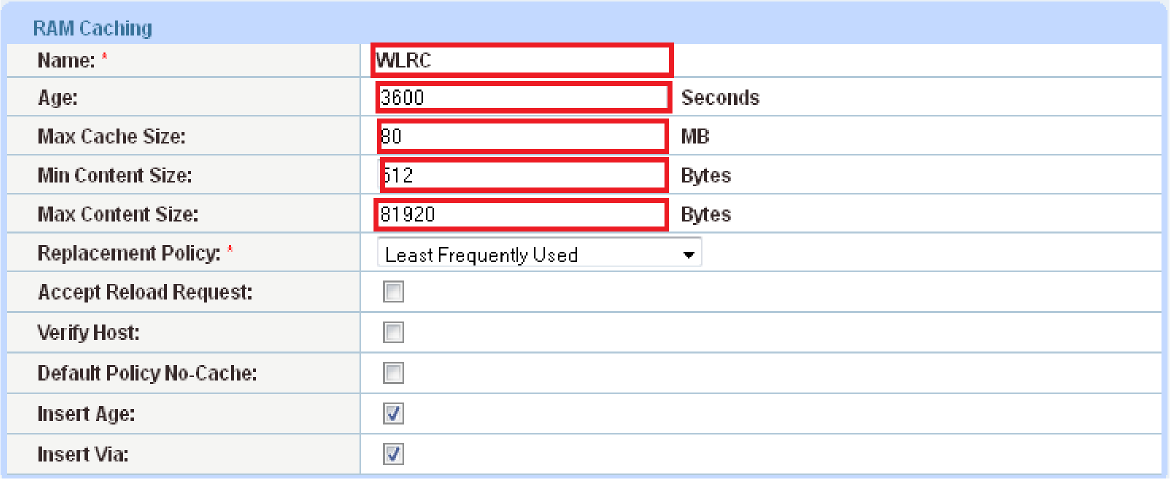
4. Enter **Age**: **“**3600”

5. Enter **Max Cache Size**: “80”

6. Enter **Min Content Size**: “512”

7. Enter **Max Content Size**: “81920”

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 policy, please refer to the “AX Series Application Delivery and Server Load Balancing Guide”.*



RAM Caching

Name: *	WLRC	
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:	□	
Verify Host:	□	
Default Policy No-Cache:	□	
Insert Age:	☑	
Insert Via:	☑	

Figure 31: RAM Caching template

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

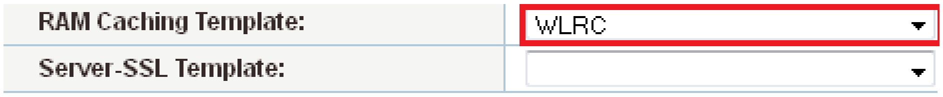
9.7.2 APPLY RAM CACHING TEMPLATE TO VIP

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

2. Click on the virtual server (VIP) name, “WLVIP”.

3. In the Port section, select the checkbox next to the port in the port list, and click **Edit**.

4. From the **RAM Caching Template** drop-down list, select the template configured above.



RAM Caching Template:	WLRC
Server-SSL Template:	

Figure 32: RAM Caching template applied to virtual port

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

9.8 HTTP TO HTTPS REDIRECT

This section of the deployment guide explains how to redirect WebLogic traffic that originates from HTTP to HTTPS using AX aFleX scripts. aFleX is based on a standard scripting language, TCL, and it enables the load balancer to perform Layer 7 deep-packet inspection (DPI). For examples of aFleX scripts, please refer to the following URL:

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

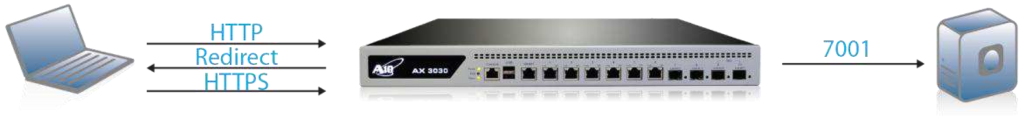


Figure 33: HTTP-to-HTTPS redirect

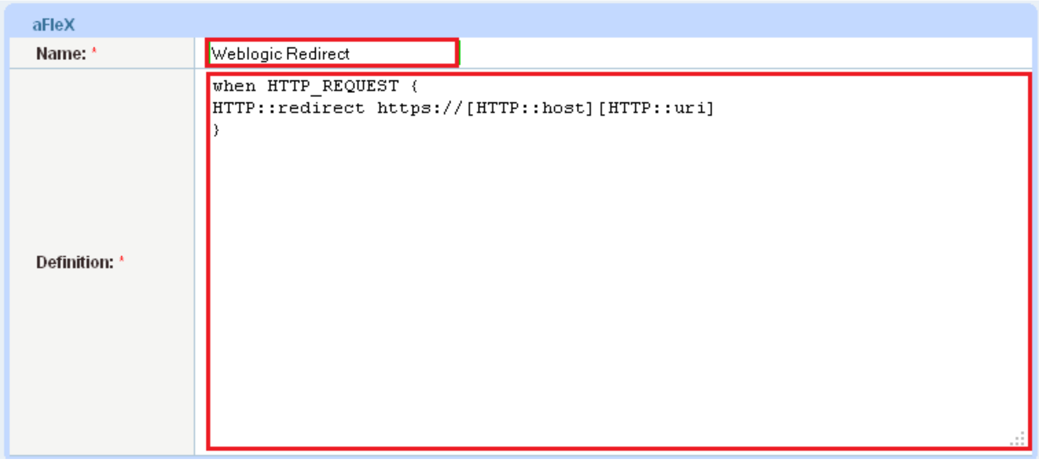
As an example, one of the most common aFleX scripts that can be used with WebLogic servers is the "HTTP redirect to HTTPS traffic". You can download additional aFleX script examples from the URL listed above:

To configure a transparent HTTPS redirect using aFleX:

1. Create the aFleX script.

2. Configure a VIP with virtual service HTTP (port 80).

3. Apply the aFleX script to the virtual port on the VIP.



aFleX

Name: * Weblogic Redirect

Definition: *

```
when HTTP_REQUEST {
HTTP::redirect https://[HTTP::host][HTTP::uri]
}
```

Figure 34: Redirect script

Redirect Script Copy and Paste:

```
when HTTP_REQUEST {

HTTP::redirect https://[HTTP::host][HTTP::uri]

}
```

Note: *The aFleX script must be bound to virtual-server port 80.*

10 SUMMARY AND CONCLUSION

The configuration steps described above show how to set up the AX Series for Oracle WebLogic Servers. By using the AX device to load balance Oracle WebLogic Servers, the following key advantages are achieved:

- High availability for WebLogic Servers to prevent website failure, meaning there is no adverse impact on user access to applications
- Seamless distribution of client traffic across multiple Oracle WebLogic Servers for site scalability
- Higher connection throughput, faster end user responsiveness, and reduced WFE CPU utilization by initiating SSL offload, HTTP Compression, RAM Caching and Connection Reuse
- Improved site performance and reliability to end users
- Transparent traffic redirection of HTTP to HTTPS

By using the AX Series Advanced Traffic Manager, significant benefits are achieved for all Oracle WebLogic 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. APPENDIX

AX Basic Configuration

```
hostname BasicWeblogic
ip address 10.0.0.10 255.255.255.0
ip default-gateway 10.0.0.1
ip nat pool "Source NAT" 10.0.0.50 10.0.0.50 netmask /24
health monitor WLHM
 method http
slb server WLWS1 10.0.0.4
   port 7001  tcp
slb server WLWS2 10.0.0.5
   port 7001  tcp
slb service-group WLSG tcp
    method least-connection
    member WLWS1:7001
    member WLWS2:7001
slb template persist source-ip srcip
slb virtual-server WLVIP 10.0.0.100
   port 80  http
      name _10.0.0.100_HTTP_80
      source-nat pool "Source NAT"
      service-group WLSG
```

```
       template persist source-ip srcip
end
```

Advanced WebLogic Configuration

```
hostname AdvancedWL
ip nat pool "Source NAT" 10.0.0.50 10.0.0.50 netmask /24
health monitor WLHM
 method http
slb server WLWS1 10.0.0.4
   port 7001  tcp
slb server WLWS2 10.0.0.5
   port 7001  tcp
slb service-group WLSG tcp
    method least-connection
    member WLWS1:7001
    member WLWS2:7001
slb template connection-reuse WLCR
slb template cache WLRC
slb template http WLC
   compression enable
slb template client-ssl WS
   cert WS
   key WS
slb template persist cookie WLCP
slb virtual-server WLVIP 10.0.0.100
   port 80  http
      name _10.0.0.100_HTTP_80
      source-nat pool "Source NAT"
      service-group WLSG
   port 443  https
      name _10.0.0.100_HTTPS_443
      source-nat pool "Source NAT"
      service-group WLSG
      template http WLC
      template cache WLRC
      template client-ssl WS
      template connection-reuse WLCR
      template persist cookie WLCP
      aflex "WebLogic Redirect"
end
```