

Deployment Guide

AX Series with Oracle Application Server



Table of Contents

DEPLOYMENT GUIDE

AX Series with Oracle Application Server

Introduction	1
Prerequisites & Assumptions	1
Configuring AX for Oracle Application Server	2
Configuring Oracle Web Server on AX	3
Configuring HTTP Health Monitor.....	3
Auto-Port Translation.....	4
Real Server Configuration	5
Service Group Configuration.....	7
Configuring Templates for Oracle Web Server	8
HTTP Template Configuration	8
TCP Proxy Template Configuration.....	9
SSL Certificate Configuration	10
Configuring Client Template.....	11
Client SSL Template Configuration	11
Configuring HTTPS Virtual Server	12
Summary and Conclusion	14

■ Introduction

This deployment guide contains configuration procedures for AX Series server load balancers to support Oracle Application Server.

Oracle Application Server is an integrated, standards-based software platform consisting of Oracle HTTP Server and OC4J (OracleAS Containers for J2EE), which deploys J2EE-based applications. Oracle Application Server Enterprise Edition is an application platform suite (APS) that offers a comprehensive solution for developing, integrating, and deploying all of your enterprise's applications, portals, and Web sites. Enterprise Edition combines robust business integration, leading J2EE performance, capabilities for enterprise portal, real-time business activity monitoring, business intelligence, identity management, and wireless deployment.

For more information on Oracle Application Server Products visit:

http://www.oracle.com/appserver/enterprise_edition.html

The AX Series with its Advanced Core Operating System (ACOS) has been designed specifically for applications such as Oracle Application Server providing better robustness in failover situations, intelligent load sharing and offloading security processing.

This guide used the AX Series 2.0.1 in routed mode and Oracle Application Server 11g.

Prerequisites & Assumptions

- A10's AX platform should be running software version 2.0 or later.
- It is assumed that users have some basic configuration familiarity with both AX and Oracle Application Server products.
- The Oracle Application Server products used in this deployment guide are Oracle Web Server, Identity Manager and Single Sign-on. As the applications are accessed by users through the Oracle Web Server, the deployment configuration below is for the Oracle Web Server.
- The AX can be configured in one armed mode or routed mode.

INTRODUCTION

■ Configuring AX for Oracle Application Server

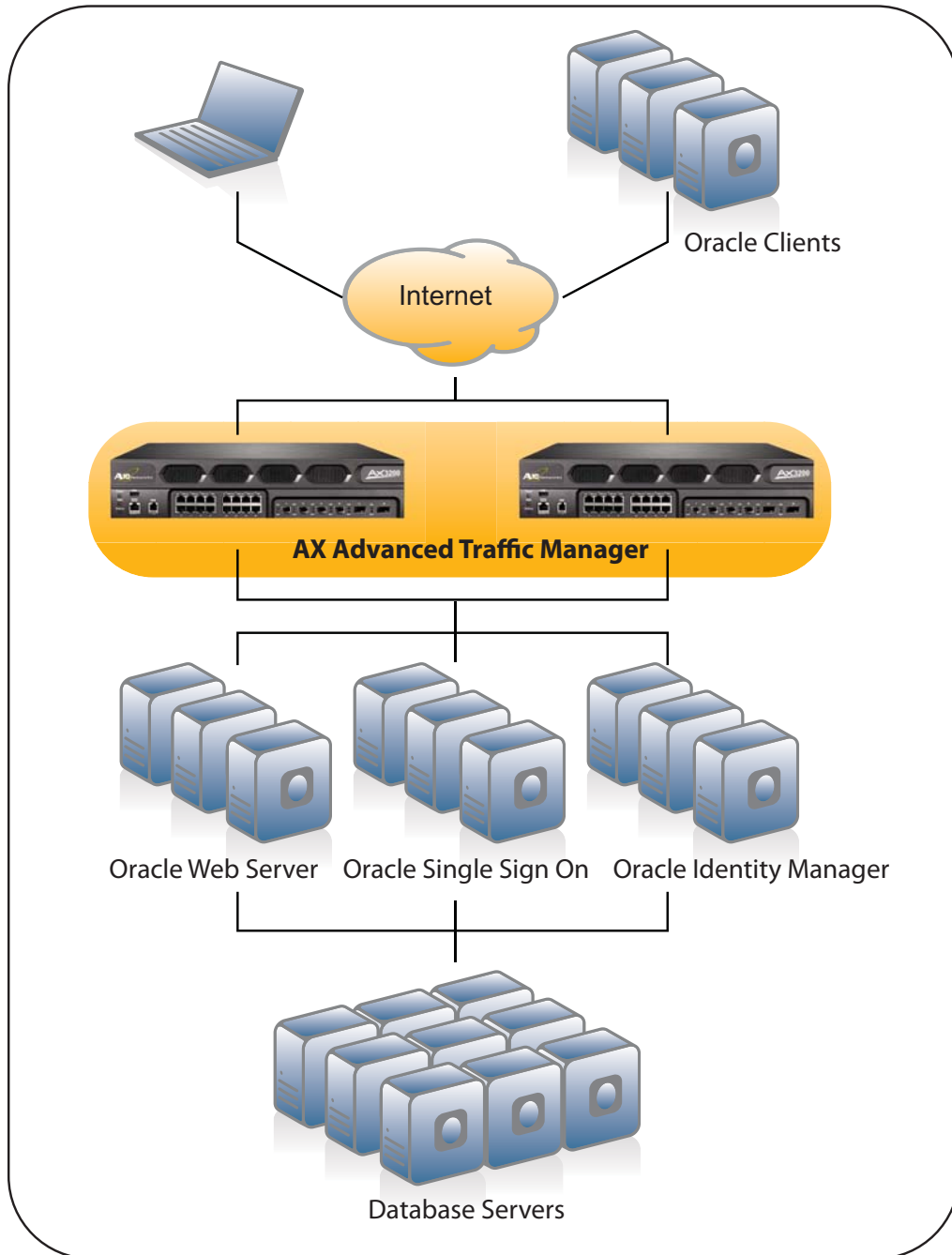


Figure 2.1 Logical deployment topology

■ Configuring Oracle Web Server on AX

Connect the AX devices to the network that consists of Oracle servers and configure the network routing entries if the servers are in a different subnet, and follow the configuration steps below.

- Configure HTTP Health Monitor
- Configure Real Server
- Configure Service Group
- Configure Template
- Configure Virtual Server

Configuring HTTP Health Monitor

To configure HTTP Health Monitor for Oracle Web Server:

1. Select **Config Mode > Service > Health Monitor**
2. Click **Add** to configure new HTTP Health Monitor
3. On the **Health Monitor** tab, enter a name for the monitor in the **Name** field. In this example, the name “*Oracle-HTTP-HM*” is used
4. In the **Method** section, select **HTTP** from the **Type** drop-down list
5. Configure optional fields as required for your deployment. In this example, the default Health Monitor settings are used
6. Click **OK** to finish configuration of the Health Monitor. The Health Monitor appears in the health monitor table

Health Monitor	
Name:	Oracle-HTTP-HM
Retry:	3
Consec Pass Req'd:	1
Interval:	30 Seconds
Timeout:	5 Seconds
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="radio"/> Text <input checked="" type="radio"/> Code

Figure 2.2 Health Monitor Configuration

Auto-Port Translation

The AX device allows you to use different port numbers for a real server port and its corresponding virtual server port. The AX auto-port translation feature can automatically translate the port numbers internally. In this example our VIP address 192.168.215.63:443 is bound with real server (192.168.215.60) port 7777, the default port for Oracle HTTP Server. The AX device translates the VIP address into the real server IP address, and translates the virtual service port number into the real service port number, to interact with the real server on the client's behalf.

Note: For standard port numbers (port numbers 0-1023), no additional configuration is required for auto-port translation. For example, if the VIP service port number is 80 and the real port number is 542, no additional configuration is required.

To configure Auto-Translate Port:

1. Select **Config Mode > Service > SLB**
2. On the menu bar, select **Global > Auto Translation**
3. Click on one of the range names. The **Auto Translation** screen appears

Note: *If a range has already been configured for use by non-standard port numbers, do not reconfigure this range. Instead, select an un-configured range.*

4. Edit the port numbers in the **Start Port** and **End Port** fields, based on the guidelines described above
5. Click **OK**

Virtual Server	Service Group	Server	Template	Global
SLB >> Auto Translation				
Auto Translation				
Range Name:		Range 2		
Start Port:		7000		
End Port:		7999		
✓ OK		✗ Cancel		

Figure 2.3 Auto-Port Translation Configurations

Real Server Configuration

In this step we configure the Real Oracle Application Server and we configure a HTTP Health Monitor on the service port.

To configure a Real Server:

1. Select **Config Mode > Service > SLB**
2. Select **Server** on the menu bar
3. Click **Add**. The **General** tab appears
4. In the **Name** field, enter a name for the server. In this example, the name is “Oracle”
5. In the **IP Address** field, enter the IP address of the server. In this example we type “192.168.216.60”
6. In the **Health Monitor** drop-down list, leave the default health monitor for layer 3, which is ping

- to the server's IP address
- 7. In the **Port** field, enter the number of the service port on the real server. In this example, the port number is "7777"
- 8. In the **Health Monitor (HM)** drop-down list for the port, select the previously configured "Oracle-HTTP-HM" Health Monitor
- 9. Click **Add** to add the port to the **Port** list for the server
- 10. Click **OK**. The real server appears in the server table
- 11. Repeat this procedure for each of the real Oracle Application servers

SLB >> **Server** >> Oracle

General

Name: * Oracle

IP Address: * 192.168.216.60

GSLB External IP Address:

Weight:

Health Monitor: (default)

Status: Enabled Disabled

Connection Limit:

Connection Resume:

Slow Start:

Server Template: default

Description:

Port

Port: * Protocol: TCP Weight(W): * No SSL

Connection Limit(CL): * Server Port Template(SPT): default

Connection Resume(CR): Health Monitor(HM): (default)

<input type="checkbox"/>	Port	Protocol	CL	CR	W	No SSL	SPT	HM
<input checked="" type="checkbox"/>	7777	TCP	1000000		1	<input checked="" type="checkbox"/>	default	Oracle-HTTP-HM

Figure 2.4 Real Server Configuration

Service Group Configuration

A Service Group contains a set of real servers from which the AX device can select to service client requests. A service group allows you to virtually support multiple servers as one logical server.

To configure a service group:

1. Select **Config Mode > Service > SLB**
2. Select **Service Group** on the menu bar
3. Click **Add**. The **Service Group** tab appears
4. In **Name** field, enter name of Service Group. In this example, the name is “*Oracle-HTTP*”
5. In the **Algorithm** drop-down list, select the preferred load-balancing method. You can control the load on each server by selecting the appropriate type of load balancing methods. For this configuration, **Round Robin** is used
6. On the **Server** drop down, select a configured real server from the drop-down list
7. In the **Port** field, enter the port “7777”
8. Click **Add**. Repeat steps 6-8 for each real server
9. Click **OK**. The new group appears in the Service Group table

Virtual Server	Service Group	Server	Template	Global
SLB >> Service Group >> Oracle-HTTP				
Service Group				
Name:	Oracle-HTTP			
Type:	TCP			
Algorithm:	Round Robin			
Health Monitor:	[Dropdown]			
Min Active Members:	<input type="checkbox"/>			
Description:	[Text Area]			
Server				
IPv4/IPv6:	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6			
Server:	Oracle	Port:	[Text Field]	
Server Port Template(SPT):	default	Priority:	1	
<input type="checkbox"/>	Server	Port	SPT	Priority
<input checked="" type="checkbox"/>	Oracle	7777	default	1

Figure 2.5 Service Group Configuration

■ Configuring Templates for Oracle Web Server

Templates are sets of configuration parameters that apply to specific service types or to servers and service ports. Even though in some cases default templates can be used, it is recommended that you create templates specifically allowing you to change the templates in the future without impacting the default templates, which others may be sharing also. For this deployment, the following types of templates are used:

- HTTP Template
- TCP-Proxy Template
- Client SSL Template

HTTP Template Configuration

1. Select **Config Mode > Service > Template**
2. Select **Application > HTTP** from the drop down menu bar. The **Template >> HTTP >> List** screen appears
3. Click **Add**. The **Template >> HTTP >> Create** screen appears
4. Enter a name for the template in the **Name** field. In our example we type “*Oracle-HTTP-Temp*”
5. Select or enter values for the template options you want to use. In this example, the default values are used for the remaining options
6. Click **OK** to finish configuration and the template now appears in the HTTP template list

Application	Connection Reuse	L4	Persistent	SSL
Template >> HTTP >> Oracle-HTTP-Temp				
HTTP				
Name: *	Oracle-HTTP-Temp			
Failover URL:	<input type="text"/>			
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"/>			

Figure 2.6 HTTP Template Configuration

TCP Proxy Template Configuration

TCP-proxy templates control TCP stack settings such as the idle timeout for TCP connections. We will use this template on a virtual server port.

To configure a TCP-Proxy template:

1. Select **Config Mode > Service > Template**
2. Click **TCP Proxy** on the top menu bar
3. Click **Add** to configure new template
4. In the **Name** field, enter a name for new template. In this example we type “*Oracle-TCPProxy*”
5. In the **Idle Timeout** field, the default value is “600” seconds but we are using “1200”. The other default settings are used in this example
6. Click **OK**

Application	Connection Reuse	L4	Persistent
Template >> TCP Proxy >> Oracle-TCPProxy			
TCP Proxy			
Name: *	Oracle-TCPProxy		
FIN Timeout:	5		Seconds
Idle Timeout:	1200		Seconds
Retransmit Retries:	3		
SYN Retries:	5		
Time Wait:	5		Seconds
Receive Buffer:	87380		Bytes
Transmit Buffer:	16384		Bytes
Initial Window Size:	<input type="checkbox"/>		
Nagle:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled		
<input type="button" value="OK"/> <input type="button" value="Cancel"/>			

Figure 2.7 TCP Proxy Template

SSL Certificate Configuration

In this section we will configure SSL Certificate for Client SSL Template. You can also import a certificate from a remote location.

To configure SSL Certificate:

1. Select **Config Mode > Service > SSL Management**
2. Click **Create**. The **SSL Management >> Certificate >> Create** screen appears
3. In the **File Name** field, type the name for the SSL certificate. In this example, the name is “Oracle-Client-SSL”
4. On the **Certificate** section there is an **Issuer** drop-down list, use the default option of **Self** from drop-down list
5. In the **Common Name** field, enter a name for the certificate. In this example we type “Oracle”
6. Fill in any additional required data and in the **Key** section select the **Key Size** from drop down list. The default is **1024 bits**
7. Click **OK**

Certificate	Cert Revocation List
SSL Management >> Certificate >> Import	
General	
Name:	Oracle-Client-SSL
Certificate	
Issuer:	Self
Common Name:	Oracle
Division:	QA
Organization:	A10Networks
Locality:	SJ
State or Province:	CA
Country:	US
E-mail Address:	oracleuser@a10networks.com
Expiration:	May 8 13:21:03 2011 GMT
Private Key	
Size:	1024 bits

Figure 2.8 SSL Certificate

Configuring Client Template

In this section we configure the Client SSL Template using the previously configured SSL certificate. As we are using a client side HTTPS and server side HTTP configuration in this Deployment Guide, we will configure these templates on the virtual server.

Client SSL Template Configuration

To configure Client SSL Template:

1. Select **Config Mode > Service > Template**
2. Select **SSL > Client SSL** from the top menu bar and drop down
3. Click **Add**. The **Template >> Client SSL >> Create** screen appears
4. In the **Name** field, enter “*Oracle-Client*” name for SSL Client Template
5. In the **Certificate Name** drop-down list, select the “*Oracle-Client-SSL*” certificate configured above
6. In the **Key Name** field, select the key configured above. In this example key is “*Oracle-Client-SSL*”
7. In the **Cache Size** field, default value is “0” but we are using “10” in this example
8. Click **OK**. The new template appears in the Client SSL template list

Application	Connection Reuse	L4	Persistent	SSL
Template >> Client SSL >> Oracle-Client				
Client SSL				
Name:	Oracle-Client			
Certificate Name:	Oracle-Client-SSL			
Chain Cert Name:				
Key Name:	Oracle-Client-SSL			
Cache Size:	20			
Pass Phrase:				
Confirm Pass Phrase:				
<input type="checkbox"/> Client Certificate Check				
<input type="checkbox"/> SSL Cipher				
<input type="button" value="OK"/> <input type="button" value="Cancel"/>				

Figure 2.9 Client SSL Template

Configuring HTTPS Virtual Server

In this step we configure a Virtual Server. We are using a secure connection so we need to select the HTTPS type for the Virtual Server and also need to bind all previously configured templates on the Virtual Server port 443 (HTTPS).

To configure a Virtual Server:

1. Select **Config Mode > Service > SLB**
2. Select **Virtual Server** on the menu bar
3. Click **Add**. The **General** tab appears
4. In the **Name** field, enter a name for the Virtual Server. In this example, the **Name** is “Oracle-VS”
5. In the **IP Address** field, enter the IP address that clients will request. In this example we use “192.168.215.63”

Virtual Server	Service Group	Server	Template	Global
SLB >> Virtual Server >> Create				
General				
Name: *	Oracle-VS	<input type="checkbox"/> Wildcard		
IP Address: *	192.168.215.63	<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			

Figure 2.10 Virtual Server Configuration

6. On the **Port** section, click **Add**. The **Virtual Server Port** tab appears
7. In the **Type** drop-down list, select **HTTPS** type for Virtual Server
8. In the **Port** field, leave “443” as the default port number for the **HTTPS** type
9. In the **Service Group** drop-down list, select the service group “Oracle-HTTP” from list

Virtual Server	Service Group	Server	Template	Global
SLB >> Virtual Server >> Port >> 443				
Virtual Server Port				
Name:	Oracle-VS			
Type: *	HTTPS			
Port: *	443			
Service Group:	Oracle-HTTP			

Figure 2.11 Virtual Server Configuration (Continuation)

10. The default **Virtual Server Port Template** is used for the service port, so leave **default** selected
11. In the **HTTP Template** drop-down list, select “*Oracle-HTTP-Temp*” template configured above
12. In the **Client-SSL Template** drop-down list, select the “*Oracle-Client*” template configured above
13. In the **TCP-Proxy Template** field, select the “*Oracle-TCPProxy*” template configured above

HTTP Template:	Oracle-HTTP-Temp
RAM Caching Template:	
Client-SSL Template:	Oracle-Client
Server-SSL Template:	
Connection Reuse Template:	
TCP-Proxy Template:	Oracle-TCPProxy

Figure 2.12 Virtual Server Configuration (Continuation)

14. Click **OK**. The port appears in the Port list of the **Port** section

Virtual Server	Service Group	Server	Template	Global
SLB >> Virtual Server >> Create				
General				
Name:	Oracle-VS	<input type="checkbox"/> Wildcard		
IP Address:	192.168.215.63	<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			
HA Group:				
Virtual Server Template:	default			
Description:				
Port				
<input type="checkbox"/>	Status	Port	Type	Service Group
<input checked="" type="checkbox"/>		443	HTTPS	Oracle-HTTP

Figure 2.13 Virtual Server Configuration (Continuation)

15. Click **OK**. The Virtual Server appears in the Virtual Server table
16. Click **Save** to save the configuration changes to the startup-config

■ Summary and Conclusion

The configuration steps described above show how to set up the AX device for Oracle Application Server. The key advantages for using AX Series in the deployment for Oracle are:

- Transparent application load sharing
 - Multiple Oracle Application Web Servers can be pooled together without any changes to how users access the applications.
- Availability
 - Obtain higher availability when Web Servers fail so that there is no direct impact to how users access the applications.
- Performance for users accessing Oracle applications using Web browser
 - Achieve higher connection throughput and faster end user responsiveness by offloading security processing to the AX device.

The AX Series Advanced Traffic Manager provides significant benefits for all users of the Oracle Application Server. For more information about AX Series products, refer to:

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

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

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

About A10 Networks

A10 Networks was founded in 2004 with a mission to provide innovative networking and security solutions. A10 Networks makes high-performance products that help organizations accelerate, optimize and secure their applications. A10 Networks is headquartered in Silicon Valley with offices in the United States, Europe, Japan, China, Korea and Taiwan. For more information, visit www.a10networks.com.

Performance by Design

To learn more about the AX Series Advanced Traffic Manager and how to improve application performance up to 8 times faster while enhancing reliability and security, visit A10 Networks' website at:

www.a10networks.com

Or call and talk to an A10 sales representative:

Corporate Headquarters

A10 Networks, Inc.
2309 Bering Drive
San Jose, CA 95131
Tel: +1 408 325-8668
Fax: +1 408 325-8666

North America Sales:

+1 888 A10-6363
+1 408 325-8616

Europe, Middle East & Africa Sales:

+31 70 799-9143

Asia Pacific Sales:

China, Beijing Office:
+86 10 8515-0698

China, Shanghai Office:
+86 21 6137-7850

Japan Sales:

+81-3-3291-0091

Korea Office:

+82-2-6007-2150
+82-2-6007-2151

Taiwan Office:

+886-2-2657-3198

