



■ **Deployment Guide**

## **Oracle PeopleSoft Enterprise 9**

# **ACOS**

**TABLE OF CONTENTS**

1 Introduction ..... 4

2 Deployment Guide Prerequisite ..... 5

3 Accessing the A10 Device Load Balancer ..... 5

4 Prerequisite Feature ..... 6

    4.1 Health Monitor Configuration ..... 6

    4.2 Source NAT Configuration ..... 7

    4.3 HTTP to HTTPS Redirect (Optional) ..... 8

    4.4 DDoS Mitigation (Optional) ..... 9

5 ACOS Optimization and Acceleration Features ..... 10

6 SSL Offload ..... 10

    6.1 HTTPS VIP Configuration ..... 10

    6.2 Import or Generate the Server Certificate ..... 11

        6.2.1 Option 1: Generate a Self-Signed Certificate ..... 11

        6.2.2 Option 2: Import the Certificate and Key ..... 13

    6.3 Configure and Apply Client SSL Template ..... 13

7 Cookie Persistence ..... 15

8 HTTP Compression ..... 16

    8.1 Create HTTP Compression Template ..... 16

9 Connection Reuse ..... 18

10 RAM Caching ..... 18

11 Load Balancing Configuration ..... 19

    11.1 Server Configuration ..... 19

    11.2 Service Group Configuration ..... 21

    11.3 Virtual Server Configuration ..... 22

11.4	Virtual Service Configuration.....	23
12	Summary and Conclusion .....	25
13	Sample Configuration.....	26

# 1 INTRODUCTION

Oracle PeopleSoft Enterprise software is the leading business processing application in the market, providing performance and security, and addressing regulatory needs through sustainable compliance. PeopleSoft is a leader in the performance management market and they have driven the market to excellence.

This deployment guide covers web tier load balancing based on WebLogic web services for Oracle PeopleSoft Enterprise suite. The Oracle PeopleSoft Enterprise Suite covers a wide range of applications, from Human Capital Management (HCM), to Financial Management (FM), Supplier Relationship Management (SRM), Service Automation, and more.

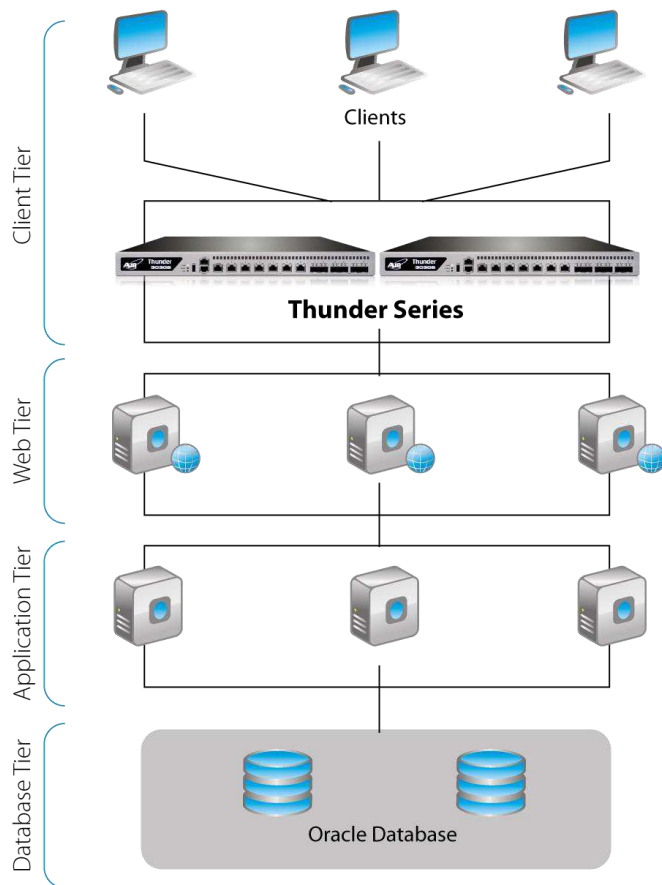


Figure 1: Oracle PeopleSoft Enterprise architecture with hardware load balancer

## 2 DEPLOYMENT GUIDE PREREQUISITE

This PeopleSoft integration has the following prerequisites:

- The A10 Networks ADC (ACOS<sup>1</sup> device) must be running ACOS version 2.7.x or higher. (While the AX Series is referred to below, a Thunder Series appliance can be used as well.)
- Oracle PeopleSoft Enterprise Applications have been tested with A10 hardware and virtual appliances.
- Oracle PeopleSoft Enterprise 9.x
- Clients tested:
  - ◆ Internet Explorer 8 or higher
  - ◆ Google Chrome 28 or higher
  - ◆ Mozilla Firefox 8 or higher

## 3 ACCESSING ACOS ON THE A10 ADC

This section describes how to access the ACOS device from a Command Line Interface (CLI) or Graphical User Interface (GUI):

- CLI – The CLI is a 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 – This is a web-based interface in which you click buttons, menus and other graphical icons to access the configuration or management pages. From these pages, you can 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)

---

<sup>1</sup> Advanced Core Operating System (ACOS) is the A10 Networks application delivery OS, running on all hardware-based and software-based Thunder Series and AX Series models,

**Note:** HTTP requests are redirected to HTTPS by default on the ACOS 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 ACOS device, see the *System Configuration and Administration Guide*.)

## 4 PREREQUISITE FEATURES

This section explains how to configure the prerequisite features to deploy an Oracle PeopleSoft Enterprise 9 load balancing solution.

### 4.1 HEALTH MONITOR CONFIGURATION

The ACOS device 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 > SLB > Server Port > Health Monitor**.
2. Select "Create" from the **Health Monitor** drop-down list.
3. In the **Name** field, enter “PSHC”.
4. In the **Method** box, Select **Type** “HTTPS”.
5. Click **OK**, then see the next section to continue with the service group configuration.

Health Monitor	
Name: *	PSHC
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:	HTTPS
Port:	443

Figure 2: Health monitor configuration

## 4.2 SOURCE NAT CONFIGURATION

This section configures the IP Address pool to be used for Source-IP Network Address Translation (SNAT). When incoming traffic from a client accesses the VIP address (for example: 192.0.2.100), the client requests are “source NAT-ed”, which means that the ACOS device replaces the client’s source IP address based on the configured address pool. The source NAT template must be applied to the virtual server port for NAT to take effect.

1. Navigate to **Config Mode> IP Source NAT > IPv4 Pool**.
2. Click **Add**.
3. Enter the following:
  - ◆ **NAT:** “SNAT”
  - ◆ **Start IP Address:** “192.0.2.200”
  - ◆ **End IP Address:** “192.0.2.200”
  - ◆ **Netmask:** “255.255.255.0”

IPv4 Pool	
Name: *	SNAT
Start IP Address: *	192.0.2.200
End IP Address: *	192.0.2.200
Netmask: *	255.255.255.0
Gateway:	
HA Group:	
IP-RR:	<input type="checkbox"/>

Figure 3: 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 source NAT template that was created in the Source NAT Pool section.

**Note:** When using the ACOS device in a High Availability (HA) configuration, an HA group must be selected. This will prevent duplicate IP addresses from occurring in the source NAT pool.

### 4.3 HTTP-TO-HTTPS REDIRECT (OPTIONAL)

This section explains how to redirect WebLogic traffic for HTTP to HTTPS using ACOS aFlex scripts. aFlex is based on a standard scripting language, TCL, and enables the ACOS device 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](http://www.a10networks.com/products/axseries-aflex_advanced_scripting.php)

As an example, one of the most commonly used aFlex scripts is the “HTTP redirect to HTTPS traffic” script. You can find the predefined aFlex script named “redirect1” for this purpose on the ACOS device. 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 type HTTP (typically, on port 80).
3. Apply the aFlex script to the virtual port on the VIP.



## 4.4 DDOS MITIGATION (OPTIONAL)

ACOS provides an additional security layer for load balanced servers and applications. Adding to an in-depth defense strategy, key protections are architected into ACOS hardware and software.

ACOS provides high-performance detection and prevention against distributed denial-of-service (DDoS) and protocol attacks that can cripple servers and take down applications. Since the ACOS device is placed between the routers and data center resources, it is ideally positioned to detect and stop attacks directed at any data center server or application. Using specialized ASICs in select models, ACOS can continue to inspect, stop, and redirect all application traffic at network speeds.

To install a standard set of DDoS Mitigation features:

1. Navigate to **Config Mode > SLB > Service > Global > DDoS Protection**.
2. Select all DDoS Protection features you would like to activate.

DDoS Protection	
<input type="checkbox"/> Drop All	<input checked="" type="checkbox"/> IP Option <input checked="" type="checkbox"/> Land Attack <input checked="" type="checkbox"/> Ping-of-Death <input checked="" type="checkbox"/> Frag <input checked="" type="checkbox"/> TCP No Flags <input checked="" type="checkbox"/> TCP SYN Fin <input checked="" type="checkbox"/> TCP SYN Frag
Out of Sequence:	<input type="text" value="10"/>
Zero Window:	<input type="text" value="10"/>
Bad Content:	<input type="text" value="10"/>

Figure 4: DDoS Mitigation

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

**Note:** Additional traffic security features are described in the *Application Access Management and DDoS Mitigation Guide*.

## 5 ACOS OPTIMIZATION AND ACCELERATION FEATURES

This section shows how to configure the ACOS device for Oracle PeopleSoft Enterprise. ACOS load balancing of PeopleSoft Enterprise traffic increases server performance and reliability with features such as SSL Offload, HTTP Compression, Connection Reuse, Cookie Persistence, and RAM Caching.

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 templates, you can bind the features to the virtual port on the VIP.

## 6 SSL OFFLOAD

### 6.1 HTTPS VIP CONFIGURATION

SSL Offload mitigates the processor-intensive impact upon web server applications or web server farms of encrypting and decrypting SSL traffic sent via secure SSL. SSL Offload is a performance optimization feature that enables a server to offload the SSL traffic to the ACOS device.

To configure SSL Offload with WebLogic, navigate to the virtual service configuration for PeopleSoft Enterprise on the ACOS device, and configure port 443 (HTTPS) on the virtual service port.

1. Navigate to **Config Mode > Service > SLB > Virtual Service**.
2. Click on the service name. In this example, "\_10.0.0.200\_HTTP\_80".
3. Select "HTTPS" from the **Port** drop-down list.

**Note:** Leave the port 80 configuration in the service group and server. SSL offload is configured as HTTPS (443) on the front end but uses HTTP (80) to the backend servers/server pool.

Virtual Service	
Virtual Service: *	_10.0.0.200_HTTP_80
Type: *	HTTP
Port: *	HTTP
Address *	HTTPS
HA Group:	Fast-HTTP
Service Group:	TCP
Connection Limit:	UDP
<input checked="" type="checkbox"/>	RTSP
<input type="checkbox"/>	FTP
<input type="checkbox"/>	MMS
Status:	SSL-Proxy
SYN Cookie:	SMTP
	SIP
	SIP-TCP
	SIP-TLS
	TCP-Proxy
	DNS-UDP
	Diameter
	TFTP
	Others

IPv4    IPv6

Logging

eferred method fails

tion fails

Figure 5: Virtual service configuration

## 6.2 IMPORT OR GENERATE THE SERVER CERTIFICATE

Since the ACOS device will act as an HTTPS proxy for the PeopleSoft web servers, the server certificate for each server must be imported onto or generated on the ACOS device.

There are two options for installing an SSL certificate on the ACOS device:

- **Option 1:** Generate a self-signed certificate on the ACOS device.
- **Option 2:** Import an SSL certificate and key signed by a Certificate Authority (CA).

### 6.2.1 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: "PS".
4. From the **Issuer** drop-down list, select "Self".
5. Enter the following values:
  - ◆ **Common Name:** "PS"
  - ◆ **Division:** "A10"

- ◆ **Organization:** "A10"
- ◆ **Locality:** San Jose
- ◆ **State or Province:** "CA"
- ◆ **Country:** "USA"
- ◆ **Email Address:** "psadmin@example.com"
- ◆ **Valid Days:** "730" (Default)
- ◆ **Key Size (Bits):** "2048"

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

<b>General</b>	
File Name: *	PS
<b>Certificate</b>	
Issuer:	Self
Common Name: *	PS
Division:	A10
Organization:	A10
Locality:	San Jose
State or Province:	CA
Country (C): *	United States of America
	US
Email Address:	psadmin@example.com
Valid Days:	730 days
<b>Key</b>	
Key Size:	2048 Bits

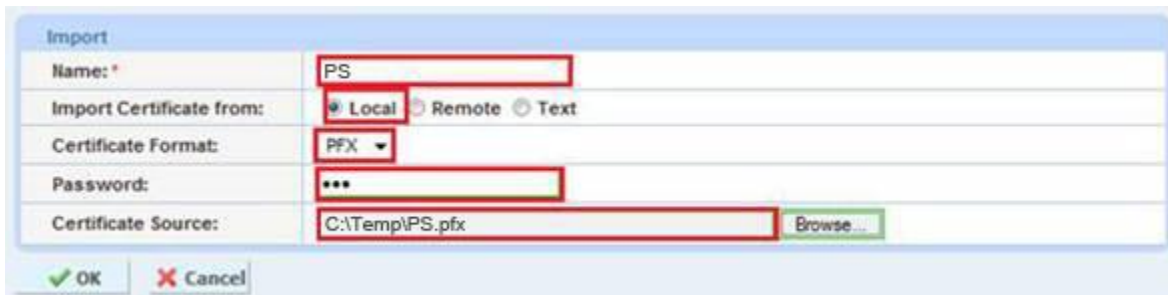
Figure 6: Self-signed certificate configuration

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

### 6.2.3 OPTION 2: IMPORT THE CERTIFICATE AND KEY

1. Navigate to **Config Mode > Service > SSL Management > Certificate**.
2. Click **Import**.
3. Enter the **Name**: "PS"
4. Select "Local" or "Remote", depending on the file location.
5. Enter the certificate Password (if applicable).
6. Enter or select file location and access settings.
7. Click **OK**.

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



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

Figure 7: SSL certificate import

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

## 6.3 CONFIGURE AND APPLY CLIENT-SSL TEMPLATE

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

1. Navigate to **Config Mode > Service > Template > SSL > Client SSL**.
2. Click **Add**.
3. Enter or select the following values:
  - ◆ **Name:** "Client SSL-PS"

- ◆ **Certificate Name:** "PS"
- ◆ **Key Name:** "PS"
- ◆ **Pass Phrase:** "example"
- ◆ **Confirm Pass Phrase:** "example"

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

Figure 8: Client-SSL template

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

4. Navigate to **Config Mode > SLB > Virtual Server**.
5. Click on the virtual server name.
6. Select "443" and click **Edit**.
7. Apply the created client-SSL template by selecting it from the **Client-SSL Template** drop-down list.
8. Click **OK**, then click **Save** to save the configuration.

## 7 COOKIE PERSISTENCE

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**: "PS"
4. Select the **Expiration** radio button and enter "86400" in the **Seconds** field.
5. Enter the **Cookie Name**: "PS"
6. Check the **Service Group**, Select "Server"

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

Figure 9: Cookie persistence template

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

## 8 HTTP COMPRESSION

HTTP Compression is a bandwidth optimization feature that compresses 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.

### 8.1 CREATE HTTP COMPRESSION TEMPLATE

1. Navigate to **Config Mode > 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: *	HTTP Compression
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 10: HTTP compression template

5. Select "Enabled" in the **Compression** field.

**Note:** ACOS offers various compression levels, ranging from levels 1 to 9. Level 1 is the recommended compression setting.



The screenshot shows a configuration window titled "Compression". It contains several settings:

- Compression:** Radio buttons for "Enabled" (selected and highlighted with a red box) and "Disabled".
- Keep Accept Encoding:** Radio buttons for "Enabled" and "Disabled" (selected).
- Level:** A dropdown menu set to "1 (least compression, fastest)", which is also highlighted with a red box.
- Min Content Length:** A checked checkbox and the value "120".
- Content Type:** A section with a "Type:" input field, a table with one row containing "Type", and "Add" and "Delete" buttons.
- Exclude Content Type:** A section with a "Type:" input field, a table with one row containing "Type", and "Add" and "Delete" buttons.
- Exclude URI:** A section with a "URI:" input field, a table with one row containing "URI", and "Add" and "Delete" buttons.

At the bottom of the window are "OK" and "Cancel" buttons.

Figure 11: Compression configuration column

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

## 9 CONNECTION REUSE

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

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

Figure 12: TCP Connection Reuse template

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

## 10 RAM CACHING

Cacheable data is cached within the ACOS device, thus reducing overhead on the PeopleSoft web servers and increasing their capacity. RAM Caching reduces the number of connections and server requests that need to be processed.

1. Navigate to **Config Mode > Service > Template > Application > RAM Caching**.
2. Click **Add**.
3. Enter or select the following values:
  - ◆ **Name**: "PSRC"
  - ◆ **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 Application Delivery and Server Load Balancing Guide.*

RAM Caching	
Name: *	PSRC
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 No-Cache:	<input type="checkbox"/>
Insert Age:	<input checked="" type="checkbox"/>
Insert Via:	<input checked="" type="checkbox"/>

Figure 13: RAM Caching template

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

## 11 LOAD BALANCING CONFIGURATION

### 11.1 SERVER CONFIGURATION

This section demonstrates how to configure the WebLogic web servers on the ACOS device.

1. Navigate to **Config Mode > SLB > Server**.
2. Click **Add** to add a new server.
3. Within the Server section, enter the following required information:
  - ◆ **Name:** "WLPS1"
  - ◆ **IP address /Host:** "192.0.2.2"
  - ◆ **Health Monitor:** "PSHC"

**Note:** Enter additional servers if necessary.

General	
Name: *	PSWS1
IP Address/Host: *	192.0.2.2 <input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
GSLB External IP Address:	
IPv6 address Mapping of GSLB:	
Weight:	1
Health Monitor:	PSHC
Status:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Connection Limit:	8000000 <input checked="" type="checkbox"/> Logging
Connection Resume:	

Figure 14: Server configuration

- To add a port to the server configuration, go to the **Port** section.
- Enter the port number in the **Port** field.
- Select the **Protocol**.
- Click **Add**.

**Port**

Port: \* 80 : Protocol: TCP Weight(W): \* 1  No SSL

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

Server Port Template(SPT): default Server-SSL Template(SST):

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

Extended Stats(ES):  Enabled  Disabled KDC Service Name(KDCSN):

	Port	Protocol	W	No SSL	CL	CR	SPT	SST	HM	ES	KDCSN
<input checked="" type="checkbox"/>	80	TCP	1	<input checked="" type="checkbox"/>	8000000		default		(default)	<input checked="" type="checkbox"/>	

Figure 15: Server port configuration

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

## 11.2 SERVICE GROUP CONFIGURATION

This section shows how to configure the service group.

1. Navigate to **Config Mode > SLB > Service Group**.
2. Click **Add**.
3. Enter or select the following values:
  - ◆ **Name:** "PSSG"
  - ◆ **Type:** "TCP"
  - ◆ **Algorithm:** "Least Connection"
  - ◆ **Health Monitor:** "PSHC"

Service Group	
Name: *	PSSG
Type:	TCP
Algorithm:	Least Connection
Auto Stateless Method:	<input type="checkbox"/>
Traffic Replication:	
Health Monitor:	PSHC
Server Template:	default
Server Port Template:	default

Figure 16: Service group configuration

4. In the **Server** section, select a server from the **Server** drop-down list and enter "80" in the **Port** field.
5. Click **Add**. Repeat for each server.

Server configuration interface showing fields for IPv4/IPv6, Server name (PSWS2), Port (80), Server Port Template (SPT) (default), Priority (1), and Stats Data (Enabled). A table lists the configured server: PSWS1 on port 80 with priority 1 and stats data enabled. Action buttons include Add, Update, Delete, Enable, and Disable.

Server	Port	SPT	Priority	Stats Data
PSWS1	80	default	1	✓

Figure 17: Server configuration

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

### 11.3 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 > SLB > Virtual Service**.
2. In the **General** section, enter the name of the VIP and its IP Address:
  - ◆ **Name:** "PSVIP"
  - ◆ **IP Address:** "203.0.113.100"

Virtual server configuration interface showing fields for Name (PSVIP), IP Address or CIDR Subnet (203.0.113.100), Status (Enabled), and Disabled on Condition (Disabled When All Ports Down).

Figure 18: Virtual server configuration

3. In the **Port** section, click **Add**.
4. Select the following values:

- ◆ **Virtual Server:** "HTTPS"

**Note:** The port number will be pre-selected after you select the service type (from the **Type** drop-down list).

- ◆ **Service Group:** "PSSG"

Virtual Server Port	
Virtual Server:	PSVIP
Type: *	HTTPS
Port: *	443 To
Service Group:	PSSG
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

Figure 19: Virtual-server port configuration

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

## 11.4 VIRTUAL SERVICE CONFIGURATION

This section of the deployment guide is where all the optimization and acceleration features can be applied to the VIP. In this example, all the optimization and acceleration features are applied to port 443 (HTTPS).

To apply the feature templates created in the previous sections:

1. Navigate to **Config Mode > SLB > Service > Virtual Server**.
2. In the Virtual Server Port section, add port 443 (HTTPS). Select the following values:
  - ◆ **Virtual Server:** "HTTPS"
  - ◆ **Port:** "443"

**Note:** The Port number will be pre-selected after you select the service type.

- ◆ **Service Group:** "PSSG"

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

Virtual Server Port	
Virtual Server:	PSVIP
Type: *	HTTPS
Port: *	443 To
Service Group:	PSSG
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
<input type="checkbox"/>	Client IP Sticky NAT

Figure 20: Virtual-server port configuration

4. Apply the pre-configured features by selecting the feature templates from the drop-down lists for each template type.

Virtual Server Port Template:	default
Access List:	
Source NAT Pool:	SNAT <input type="checkbox"/> Auto
aFlex:	<input type="checkbox"/> Multiple
HTTP Template:	HTTP Compression
RAM Caching Template:	PSRC
Client-SSL Template:	Client SSL-PS
Server-SSL Template:	
Connection Reuse Template:	PCConnectionReuse
TCP-Proxy Template:	
Persistence Template Type:	Cookie Persistence Template
Cookie Persistence Template:	PS
WAF:	
HTTP Policy:	
External Service Template:	
Authentication Template:	
Policy Template:	

Figure 21: HTTPS features

5. Click **OK** and **Save** the configuration.



## 12 SUMMARY AND CONCLUSION

The sections above show how to deploy ACOS to optimize the Oracle PeopleSoft Enterprise Suite. By using ACOS to load balance a pool of Oracle PeopleSoft Enterprise web servers, the following key advantages are achieved:

- High availability for PeopleSoft Web Servers to prevent application failure
- Seamless distribution of client traffic across multiple PeopleSoft Web Servers to provide scalability
- Higher connection counts, faster application responsiveness, and reduced PeopleSoft Web Server CPU utilization through use of SSL Offload, HTTP Compression, RAM Caching and Connection Reuse
- Improved application performance and reliability for end-users

By using the ACOS Application Delivery Controller, significant benefits are achieved for all PeopleSoft Web Server users. For more information about ACOS products, please refer to the following URLs:

<http://www.a10networks.com/products/thunder-series.php>

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

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

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

## 13 SAMPLE CONFIGURATION

```
ip nat pool SNAT 203.0.2.100 203.0.2.100 netmask /24

health monitor PSHC

  method http

slb server PS1 192.0.2.2

  health-check PSHC

  port 80 tcp

slb server PS2 192.0.2.3

  health-check PSHC

  port 80 tcp

slb service-group PSSG tcp

  method least-connection

  health-check PSHC

  member PS1:80

  member PS2:80

slb template connection-reuse PCConnectionReuse

slb template cache PSRC

slb template client-ssl "Client SSL-PS"

  cert PS

  chain-cert PS

  key PS pass-phrase encrypted
KZlpUbp6Q888EIy41dsA5zwQjLjV2wDnPBCMuNXbAOc8EIy41dsA5zwQjLjV2wDn

slb template persist cookie PS

  name PS

  expire 86400

  match-type server service-group

slb virtual-server PSVIP 203.0.113.100
```

```
port 443 https
  name _203.0.113.100_HTTPS_443
  source-nat pool SNAT
  service-group PSSG
  template cache PSRC
  template client-ssl "Client SSL-PS"
  template connection-reuse PCConnectionReuse
  template persist cookie PS
end
```