

# **Configuring Secure Oracle E-Business Suite 11i Deployment Using Cisco Application Control Engine (ACE)**

This document contains information for implementing SSL with Oracle E-Business Suite 11i. It provides guidance for a successful implementation and covers specific steps for configuring Oracle E-Business Suite using the SSL offload feature of the Cisco Application Control Engine (ACE) and various E-Business Suite application components such as Oracle HTTP Server and Forms Server.

The following sections are discussed:

- Prerequisites and Configuration Notes
- ACE SSL Offload Feature
- ACE and Oracle E-Business Suite Application Configuration Details
  - HTTP Load Balancing
  - Configuring ACE for SSL
- References

#### Acronyms

- EBS—(Oracle) E-Business Suite
- OAM—Oracle Applications Manager
- ACE—(Cisco) Application Control Engine
- ANM—(Cisco) Application Networking Manager
- CLI—Command Line Interface
- VIP—Virtual IP



# **Prerequisites and Configuration Notes**

The following requisites and configurations are available for noteworthy consideration.

- Oracle EBS installation of version 11.5.10 or higher with latest recommended patches
- Oracle EBS environment should be AutoConfig enabled
- Cisco ACE (version 2.1 or greater) must be configured in the network. Refer to detailed configuration procedures outlined in following document:

http://www.cisco.com/en/US/docs/interfaces\_modules/services\_modules/ace/v3.00\_A2/configurat ion/slb/guide/slbgd.pdf

- The connection from the client to ACE (SSL termination device) is HTTP over SSLv3/TLS (HTTPS); The ACE is configured to listen on TCP Port 443 for secure connections (HTTPS)
- The backend connection from ACE to Oracle Application Server is clear-text (HTTP); The Oracle
  application server is listening on TCP port 8000 for non-secure connections
- The load balancer (also acting as SSL accelerator) is doing port translation from TCP 443 on the front-end client side to TCP 8000 on the server-side application host
- Oracle Forms must be configured in servlet mode. For detailed information on configuring Oracle forms in servlet mode, please refer to Oracle Metalink ID 201340.1:

http://metalink.oracle.com/metalink/plsql/ml2\_documents.showFrameDocument?p\_database\_id=NOT&p\_id=201340.1

# **ACE SSL Offload Feature**

The integrated SSL (HTTPS) capabilities of the ACE allow for secure E-Business Suite transactions. The ACE provides hardware-based SSL acceleration, moving this processor-intensive functionality from the CPU or NIC of the server into the network. Centralized SSL services in the network allow secure transactions to be efficiently processed and inspected by other network-based services, such as IDS and IPS.

# ACE and Oracle E-Business Suite Application Configuration Details

The remainder of this document outlines the application environment, including detailed instructions for implementing load balancing for Oracle EBS environments using Cisco ACE. This section also details modifications required for enabling:

- HTTP/HTTPS load balancing and session persistence
- Forms listener servlet (a pre-requisite required to enable HTTPS)
- SSL accelerator

The Oracle tool AutoConfig manages changes in the Oracle applications systems using an application context file. The context file uses an XML format and represents the application environment on a single node. The context file can be modified by leveraging Oracle Applications Manager (OAM) through a set of configuration wizards. Modifications made through OAM will be reflected in the environment only after running AutoConfig using the **adautocfg** script that is supplied by the software. Figure 1 shows an overview of the application and database nodes along with their status as reported by OAM.

Figure 1 shows the Oracle Applications Manager Dashboard



urity ent Processing	Naviga Forms	te to Appl	ication Services	
urity ent Processing	Forms	Web		
ent Processing	Forms	Web		
ent Processing	Forms	Web		
ent Processing	Forms	Web		
11 III				
	0	0		
	~	~		
Ø				
8				
	~	~		
	×	×		
	~	~		
	8	8		
erts				
ed: 08-04-2008 15	10:13	0		
	Et Et	0		
91	**************************************	x x x x x x x x x x x x x x x x x x x		

The following configurations are detailed:

- HTTP Load Balancing
- Configuring ACE for SSL

# **HTTP Load Balancing**

I

Figure 2 shows how the hardware load balancer distributes connections across the multiple web nodes.

Figure 2 Load Balancing Connections







Hardware-based HTTP load balancers must be configured to ensure persistent session connections between clients and Web Server Nodes in Oracle E-Business Suite 11i environments. Maintaining session persistence is essential to ensure that a user session remains on the same middle tier throughout the duration of the session. If the session is not maintained, the users may experience a "Lost transaction context" message. For additional details please refer to Oracle Metalink node ID 456906.1: (http://metalink.oracle.com/metalink/plsql/ml2\_documents.showFrameDocument?p\_database\_id=NO T&p\_id=201340.1).

The following HTTP load balancing configurations are provided:

- Configuring Application Web Nodes to Use Cisco ACE as Load Balancer for EBS 11i, page 4
- Configuring Server Load Balancing Policy in ACE Using ANM, page 6
- Configuring Session/Cookie Persistence in ACE Using ANM, page 7
- Creating the HTTP Health Probe Using ANM, page 8
- Enabling Forms Servlet, page 9
- Enabling SSL Accelerator, page 12
- Configuring the Virtual IP (VIP) on ACE using ANM, page 14

## Configuring Application Web Nodes to Use Cisco ACE as Load Balancer for EBS 11i

The following procedure is used to configure Application Web Nodes to use Cisco ACE as load balancer for EBS 11i.

I

- Step 1Log in to the Oracle Applications Manager as shown in Figure 3 and select the Site Map System<br/>Administration tab, then select AutoConfig.
- Step 2 Click Launch Wizards.
- **Step 3** Enable HTTP Load Balancing (Figure 3).

#### 🛢 dcap-lr-controller-1 - Remote Desktop - 8 × Cracle Applications Manager - Microsoft Internet Explorer Edit View Favorites Tools Help Eile 🕒 Back + 🕤 - 💌 😰 🧖 🔎 Search 💏 Favorites 🐵 🗇 + 🗽 🗹 + 🥃 🛍 Agdress 🖗 https://wwwin-cefin.gsb.dcap.com/8000/oa\_servlets/weboam/adornfigladv/adv/GODptions\$target=OEFIN\$finctNm=A0\*\_AD\*\_CONFIG 🔽 🛃 Go 🛛 Links 🍟 🖕 Snagit 🔁 🛫 ORACLE ()) ()) R ? () Applications Manager rt Cart Setup Home Logout Help Applications Dashboard | Site Map Applications System:OEFIN > AutoConfig **Configuration Wizards** Configuration Name Description Resources HTTP Load balancing Suite Release 11 system if you have a third party HTTP load balancer. Use this option to also disable HTTP Load Balancing. Enable Disable (i) Information Please setup your Metalink Credentials to view external Use this option to configure SSL for an E-Business Suite Release 11i Enable Disable SSL resources. system. Use this option to configure an E-Business Suite Release 11i system Enable Disable with a SSL accelerator. SSL Accelerator Forms Listener Servlet Use this option to enable or disable the Forms Listener Servlet for an Enable Disable E-Business Suite Release 11 i system. Apache JServ load Use this option to enable or disable Apache Jserv Load Balancing across multiple Web nodes for an E-Business Suite Release 11 i Apache JServ load balancing system. Related Links Verify Configuration Wizards Infrastructure Add to Support Cart Support Cart | Setup | Home | Logout | Help Copyright 2001, 2006 Oracle Corporation. All Rights Reserved. About Oracle Applications Manager Version 2.3.1 📄 📄 🙆 Internet 🔊 Start 🛛 🚱 🧶 🛛 🖗 Oracle Applications M... **S**∎ ♥ 9

Figure 3 Enabling HTTP Load Balancing in Oracle Application Manager.

- **Step 4** Select the nodes to be included as real servers in the ACE server farm configuration.
- **Step 5** Provide the information for the following variables as shown in Figure 4 so that Oracle apps will create well-formed URLs.
  - **s\_webentryhost** DNS name of the ACE VIP (eg: wwwin-oefin)
  - t\_session\_persistent Check this box if you will be using cookie-based stickiness
  - s\_webentrydomain Domain name associated with VIP
  - s\_webentryprotocol Select https

I

• s\_active\_webport - default value is 8000; Can be customized to user's choice

#### Figure 4 Configuring HTTP Load Balancer Variables in Oracle Applications Manager

dress https://	www.in-oefin.osh.dcan.com:8000/	na servlets/webnam/nam/adconfin/adv/adv/fdW	//zard\$index=0\$action=Enable\$target=0EEIN\$test=r▼ 📑 Go Links » 🍒 Spaolt 🗮 🖭
IEI undestill	initial contriguences presidences of	og_on modynessenitisenitiseningten version	
Applica	ations Manager	n/s-1	Support Cart Selue Home Loacut Hele
Applications D	lashboard   Site Map		
		Nodes Parameters(1) Parameter	ers(2) Validation Confirmation
TTP Load b	alancing:Enable:Para	imeters(1)	
itle	Parameter Name	Value	Description
eb Host entry iint	s_webentryhost	wwwin-oefin	The host name of the HTTP load balancer from which all incoming http requests are distributed.
	t_session_persistent		Check if HTTP load balancer supports session-persistent client connections
	t_dns		Check if DNS Layer load balancing is in use.
	s_webentrydomain	gslb.dcap.com	The HTTP load-balancer's domain name
/eb domain ntry point	s webentryurinrotocol	http 💌	This Web entry protocol. Acceptable values for this parameter are http or https.
/eb domain ntry point /eb entry rotocol			
/eb domain htry point /eb entry rotocol ctive Web Port	s_active_webport	8000	The Active Web port should be set to the HTTP load-balancer's external port.

- **Step 6** At this point, a series of validation and confirmation panels will be displayed. After successfully completing these steps, basic load balancing configurations will be saved on the context files of each server node selected.
- Step 7 Stop the application services (using the adstpall.sh script) on each of the application nodes.
- **Step 8** Run the **autocfg** script on the respective application nodes and verify the log files to ensure there are no errors.
- **Step 9** Restart the application services using the **adstrtal.sh** script and verify that the load balancer is distributing the connections.

# **Configuring Server Load Balancing Policy in ACE Using ANM**

The following procedure is used to configure server load balancing policy in ACE using ANM.

- **Step 1** Select the predefined server farm as shown in Figure 5.
- Step 2 Select the Predictor tab and choose a predictor Type (the default is Roundrobin).



#### Figure 5 Configuring Load Balancing in ACE Using ANM

#### **Configuring Server Load Balancing Policy Using ACE CLI**

```
serverfarm host ORACLE_APPHOSTS
predictor roundrobin
probe ORACLE_DB_CHECK
rserver ORACLE_APPHOST_1
    inservice
    rserver ORACLE_APPHOST_2
    inservice
    rserver ORACLE_APPHOST_3
    inservice
```

For additional documentation on SLB policies, please refer to the following section of the configuration guide:

http://www.cisco.com/en/US/docs/interfaces\_modules/services\_modules/ace/v3.00\_A2/configuration/s lb/guide/rsfarms.html#wpmkr1003481

## Configuring Session/Cookie Persistence in ACE Using ANM

The following procedure is used to configure session and cookie persistence in ACE using ANM.

- Step 1 Configure the appropriate sticky Group Name as shown in Figure 6.
- **Step 2** Define a name for the HTTP cookie.
- Step 3 Enable HTTP cookie insert by checking the box Enable Insert.
- Step 4 (Optional) Enable the cookie to be a session cookie by checking the box Browser expire.
- **Step 5** Assign a Sticky Server Farm to the sticky group.

#### Figure 6 Configuring Cookie Sticky Using ANM

Appl	ication Networking Manager 1.2 (0)	
@	🔓 Config 🔣 Monitor 🧮 Admin	
y 🗢 Global 🗢 Tools		
Config >Device	s>Load Balancing>Stickiness	1
Stickiness		
* 🍞 Group Name:	GROUP_1	
* Type:	Http_cookie	
* Cookie name:	ACE_COOKIE	-
	🔽 Enable Insert	
	Rowser expire	
Offset:	0	
Length:		
Secondary Name:		-
<ul> <li>Sticky Server Farm:</li> </ul>	ORACLE_APPHOSTS	
Backup Server Farm:	•	
	🔽 Replicate	
Timeout:	720	b
		1020

#### **Configuring Session Cookie Persistence Using CLI**

sticky http-cookie ACE\_COOKIE\_ORACLE GROUP\_1
 cookie insert browser-expire
 replicate sticky
 serverfarm ORACLE\_APPHOST

For additional documentation on how to configure Cisco ACE for session persistence, refer to following section of the documentation listed below.

http://www.cisco.com/en/US/docs/interfaces\_modules/services\_modules/ace/v3.00\_A2/configuration/s lb/guide/sticky.html#wpmkr1086901

## **Creating the HTTP Health Probe Using ANM**

The procedure below for setting up health monitors for the Oracle application nodes is optional, but highly recommended. From the ANM config screen shown in Figure 7, follow the steps listed below.

- **Step 1** Define a name for the health probe. In this example, the name is defined as ORACLE\_DB\_CHECK.
- **Step 2** Choose HTTP for the probe Type.
- **Step 3** (Optional) Provide a description for the health probe.
- **Step 4** Assign a Probe Interval value (set to 2 seconds here).
- **Step 5** Assign a probe Pass Detect Interval value (set to 2 seconds here).
- **Step 6** Assign a probe Fail Detect value (set to 2 seconds here).
- **Step 7** Assign a Port number. In this example, the Port is configured to 8000.
- Step 8 (Optional, but necessary for this example) Provide a User Name and Password that the probe will pass to the monitored URL (defined in Step 9) for health verification.

1

**Step 9** Define the Request HTTP URL. In this example, the EBS Login URL is supplied to ensure the application is available by logging in using the credentials defined in Step 8, above.

🤉 Global 🗢 Too		
Lonrig > Device	ss >Load Balancing >Health Monitoring	
%Name -	ORACLE_DB_CHECK	
* Type:		
Description:		
Duck - Takawal		
Probe Interval:	12	
Pass Detect Count:		
Pass Detect Interval:	2	
Receive Timeout:		
Fail Detect:	2	
Dest IP Address:		
Port:	8000	
Open Timeout:		
Ucer Name:		
oser wante.	jsysadmin	
Password:		
Expect Regex:		
Expect Regex Offset:		
	🗆 Hash	
Request Method Type:	C N/A C Head . Get	
Request HTTP URL:	/oa_servlets/AppsLogin	

#### Figure 7 Creating the HTTP Health Probe Using ANM

#### **Creating the HTTP Health Probe Using ACE CLI**

probe http ORACLE_DB_CHECK
port 8000
interval 2
faildetect 2
passdetect interval 2
credentials sysadmin sysadmin
request method get url /oa_servlets/AppsLogin
For additional documentation on creating health probes, please refer to the following section of ACE
configuration guide.

http://www.cisco.com/en/US/docs/interfaces\_modules/services\_modules/ace/v3.00\_A2/configuration/s lb/guide/probe.html#wp1030892

## **Enabling Forms Servlet**

I

The forms listener servlet is necessary in order to enable Oracle applications to use HTTPS. The servlet mode allows the user to access forms via the web server. The following procedure is required to enable the forms listener servlet.

**Step 1** Log in to the Oracle Applications Manager and select the **Site Map - System Administration** tab, then select **AutoConfig**.

- Step 2 Click Launch Wizards.
- **Step 3** Click on the **Enable Forms Listener Servlet** button as shown in Figure 8.

#### Dracle Applications Manager - Microsoft Internet Ex - 8 1 🔾 Back 🔹 🔿 🕝 😰 🐔 🔎 Search 🤹 Favorites 🔗 😥 🖏 🖓 🛄 - 🌄 🚉 Address 😰 https://www.n-oefin.gslb.dcap.com/oa\_servlets/weboam/oam/adconfig/adv/advCfgOptions\$target=OEFIN\$fncthm=AD\*\_AD\*\_CONFIG 💌 🛃 Go 🛛 Links 🎽 🍃 Snagilt 📆 🛃 ORACLE 3 1 (1) (7) Applications Manager Support Cart Setup Home Logout Applications Dashboard | Site Map ations System OEFIN AutoConfig **Configuration Wizards** Configuration Name Description Resources Action HTTP Load balancing Use this option to configure HTTP Load Balancing for an E-Business Suite Release 11 system if you have a third party HTTP load balancer. Use this option to also disable HTTP Load Balancing. Enable Disable (i) Information Please setup your Metalink Credentials to view external resources. Use this option to configure SSL for an E-Business Suite Release 111 Enable Disable SSL Use this option to configure an E-Business Suite Release 111 Enable Disable with a SSL accelerator. SSL Accelerator Forms Listener Servlet Use this option to enable or disable the Forms Listener Servlet for a Enable Disable E-Business Suite Release 11i system. Use this option to enable or disable Apache Jserv Load Balancing across multiple Web nodes for an E-Business Suite Release 11i system. Enable Disable Apache JServ load balancing Related Links Verify Configuration Wizards Infrastructure Add to Support Cart Support Cart | Setup | Home | Logout | Help Copyright 2001, 2006 Oracle Corporation. All Rights Reserved. <u>About Oracle Applications Manager Version 2.3.1</u> 265989

#### Figure 8 Configuring Forms Servlet using OAM

- **Step 4** Select the application server nodes that will be using the forms listener servlet.
- **Step 5** Set the Forms Servlet URL variable (**s\_forms\_servlet\_serverurl**) to the value /**forms/formservlet**, as shown in Figure 9.

**Step 6** Ensure the Forms Servlet Comment variable (**s\_forms\_servlet\_comment**) is blank.

I

ſ

#### *Figure 9 Enabling Forms Listener Servlet Parameters*

dcap-lr-contr	roller-1 - Remote Desktop		
Oracle Applicat	ions Manager - Microsoft Intern	et Explorer	
le <u>E</u> dit ⊻iew	Favorites Tools Help		
Back • 🕤 •	💌 💈 🎧 🎤 Search 👷 Fav	orites 😸   🖾 • 🎲 🋄 • 🖵 🕰	
dress 🦉 https:,	//www.in-oefin.gslb.dcap.com:8000/oa	_servlets/weboam/oam/adconfig/adv/advCfg	Wizard\$index=3\$action=Enable\$target=OEFIN\$test=r 🗾 🔁 Go 🛛 Links 🌋 😓 SnagIt 🖳 🛅
DRACLE			
Applic	cations Manager		Support Cart Setup Home Logout Help
Applications	Daabbaard   Site Man		
Applications	pashovaru   Site Map		
		Nodes Parameters(1) Parame	ters(2) Validation Contirmation
orms Liste	ner Servlet:Enable:Para	meters(1)	
itle	Parameter Name	Value	Description
forms Servlet JRL	s_forms_servlet_serverurl	/forms/formservlet	Forms Servlet URL
forms Servlet Comment	s_forms_servlet_comment		Forms Servlet Comment
TIP It is reco	mmended that this E-Business ad balancing is enabled. Otherw	Suite 11i instance is also configured v se, the Forms requests will not be loa	vith a) HTTP Load balancing that supports client session-persistent connections, or b) id-balanced across multiple Forms nodes
			Add to Summart Cast
			Add to Support Cart Carteer Back Step 2 015 Next
		Support Cart   Setup	Home   Logout   Help
opyright 2001, 20 bout Oracle Appli	U6 Oracle Corporation. All Rights Rese cations Manager Version 2.3.1	rved.	

Figure 10 Validating Forms Listener Servlet Parameters

		* 1 01	CONSIST.		
le <u>E</u> c	dit View Favorites	s Loois Help			<b>//</b>
Back	• 🖸 • 💌 🖬 🖠	🞧 🎾 Search 😚 Favorites	🛞   🎯 • 😓 🔟 • 📘	, iQ,	
dress	e https://wwwin-oe	fin.gslb.dcap.com:8000/oa_servk	ets/weboam/oam/adconfig/a	dv/advCfgWizard\$index=3\$action=Enable\$t	arget=OEFIN\$test=r 🗾 🔂 Go 🛛 Links 🦥 🍃 SnagIt 🔁 🛅
Арр	lications Dashboar	d   Site Map			
					0
				Parameters(2) Validation Confi	mation
	n Lintanar Sar	ulat:Enable:Paramete	vro/2)		
orm	All Colleges Al	viet. Enable.1 al amete	(13(2)		
<u>=xpar</u>	id All   Collapse Al				
¥			0		
ocus	Title	Parameter Name	Current Value	New Value	Description
Φ	V DCAP-DCA- ORAAPP01				Web,Form
	Forms Servlet URI	s_forms_servlet_serverurl	/forms/formservlet	/forms/formservlet	Forms Servlet URL
	Forms Servlet Comment	s_forms_servlet_comment			Forms Servlet Comment
Ф	▼ DCAP-DCA- ORAAPP02				Web,Form
	Forms Servlet URL	s_forms_servlet_serverurl	/forms/formservlet	/forms/formservlet	Forms Servlet URL
	Forms Servlet Comment	s_forms_servlet_comment			Forms Servlet Comment
Ф	ORAAPP03				Web,Form
	Forms Servlet URL	s_forms_servlet_serverurl	/forms/formservlet	/forms/formservlet	Forms Servlet URL
	Forms Servlet	s_forms_servlet_comment			Forms Servlet Comment

**Step 7** At this point, a series of validation and confirmation panels will be displayed (Figure 10). After successful validation, the forms servlet configurations will be saved on the context files of each server node selected.

- **Step 8** Stop the application services (./adstpall.sh) on each of the application nodes.
- **Step 9** Run **autocfg** on the respective application nodes and verify the log files to ensure there are no errors.
- **Step 10** Restart the application services using the **adstrtal.sh** script and verify that the forms are opened in servlet mode.

# **Enabling SSL Accelerator**

The SSL accelerator wizard configures the Oracle 11i application environment to use the Cisco ACE as the external device for encryption services and server offload. The following procedure summarizes how to enable SSL acceleration using Oracle Applications Manager.

- **Step 1** Log in to the Oracle Applications Manager and select the **Site Map System Administration** tab, then select **AutoConfig**.
- Step 2 Click Launch Wizards.
- Step 3 Click on the Enable SSL Accelerator button as shown in Figure 11.

Figure 11 Enabling SSL Accelerator Using OAM

					in pre-		STORE OF
Application	ns Manager		1	(\$E)	B	R	2
11			Support Cart	Setup	Home	Logout	Help
Applications Dashbo	ard   Site Riap						
Configuration Wiz	ands						
Configuration Name	Description	Action	Resources				
ITTP Load balancing	Use this option to configure HTTP Load Balancing for an E-Business Suite Release 11i system if you have a third party HTTP load balancer. Use this partice to see disable HTTP Load Balancing	Enable Disable	Information				_
SSL	Use this option to configure SSL for an E-Business Suite Release 11i system.	Enable Disable	Credentials to view external resources.				
SSL Accelerator	Use this option to configure an E-Business Suite Release 11i system with a SSL accelerator.	Enable isable					
Forms Listener Servlet	Use this option to enable or disable the Forms Listener Servlet for an E-Business Suite Release 11i system.	Enable Disable					
Apache JServ load balancing	Use this option to enable or disable Apache Jserv Load Balancing across multiple Web nodes for an E-Business Suite Release 11i system.	Enable Disable					
Related Links							
erify Configuration Wi	zards Infrastructure						
				Add	to Sup	port Ca	rt
	Sunnert Cart   Setun   Home	Lonout L Help					
opyright 2001, 2006 Oracle	e Corporation. All Rights Reserved.	Profession 1 Fische					

- **Step 4** Click on application nodes using the SSL Accelerator service.
- **Step 5** Provide the information for the following variables, as shown in Figure 12 and Figure 13, so that the Oracle applications will create well formed URLs.
  - s\_webentryhost DNS name of the ACE VIP (eg: wwwin-oefin)
  - s\_webentrydomain Domain associated with the ACE VIP
  - **s\_webentryurlprotocol** Set to **https**.
  - **s\_active\_webport** Change this to a value of your choice, or 443, which is the default well-known HTTPS port value

• **s\_webssl\_port** – Change this to a value of your choice, or 443, which is the default well-known HTTPS port value

#### Figure 12 Enable the SSL Accelerator

L

Γ

ORACLE			
Applic	ations Manager		Support Cert Setup Home Logout Help
Applications	Dashboard   Site Map		
		Nodes Parameters(1) Parameter	s(2) Validation Confirmation
SSL Acceler	ator:Enable:Paramete	rs(1)	
itle	Parameter Name	Value	Description
Veb Host entry ∞int	s_webentryhost	www.in-oefin	The SSL accelerator's host name.
Web domain entry point	s_webentrydomain	dcap.com	The SSL Accelerator's domain name
Active Web Port	s_active_webport	443	The Active Web port should be set to the SSL accelerator's external interfacing port.
	t_ssl_accelerator	M	SSL accelerator is in use.
JRL Protocol	s_url_protocol	http	URL Protocol
Local URL Protocol	s_local_url_protocol	http	Local URL Protocol
Neb entry protocol	s_webentryurlprotocol	https	Web entry Protocol
TIP Note that the E-Bus Deployme	the URL protocol, Local URL iness Suite Release 11i with ents of E-Business Suite 11i;	. protocol, and Web entry protocol are set a SSL Accelerator, please see the Oracle N and the Oracle MetaLink Note 123718.1 -	automatically to the values shown above. For additional information on configuring detaLink Note 217368.1 - Advanced Configurations and Topologies for Enterprise A Guide to Understanding and Implementing SSL with Oracle Apolications 11i.

#### Figure 13 Enable the SSL Accelerator

Oracl	e Applications Man	ager - Microsoft Internet I	xplorer		-14
ile E	dit Vjew Favorite	is Iools Help			
Back	· 0 - N 2	Search 📌 Favorit	es 🙆 🙆 • 🚴 🖬 •		
trace	bitner //www.in.ou	afin orth dean comi9000/op.ca	n late i wako am lo am la deonfia i	adu/adu/fallinaudtindau=2tartinn=Ensh	left weath OFFINItiester - 💌 🖾 Go 🛛 Links 🎽 💪 Spanit 🐻 🖻
20.000	Tel neto://www.ro	enn syster acap.com.boooyaa_se	r necs/webban (ban yaucor ing)	aurfaurci ymzaropi idex=zgacion=chac	
Ари	lications Dashbo	ard   Site Map			
	and the second se		0 0		0
			Notes Pathemeters(1)	Parameters(2) Validation Co	Infimation
				Fundation (2)	
SSL	Accelerator:E	nable:Parameters(2	)		
Expan	nd All Collapse A	11			
¢					
Focus	Title	Parameter Name	Current Value	New Value	Description
	Vodes				
¢	DCAP- DCA- ORAAPP02				Web,Form
	Web Host entry point	s_webentryhost	wwwin-oefin	wwwin-oefin	The SSL accelerator's host name.
	Web domain entry point	s_webentrydomain	gslb.dcap.com	dcap.com	The SSL Accelerator's domain name
	Active Web Port	s_active_webport	8000	443	The Active Web port should be set to the SSL accelerator's external interfacing port.
		t_ssl_accelerator			SSL accelerator is in use.
	URL Protocol	s_url_protocol	http	http	URL Protocol
	Local URL Protocol	s_local_url_protocol	http	http	Local URL Protocol
	Web entry	s_webentryurlprotocol	https	https	Web entry Protocol

- **Step 6** At this point a series of validation and confirmation panels will be displayed. After successfully completing these steps, basic load balancing configurations will be saved on the context files of each server node selected.
- Step 7 Stop the application services (using the adstpall.sh script) on each of the application nodes.
- **Step 8** Run the **autocfg** script on the respective application nodes and verify the log files to ensure there are no errors.
- **Step 9** Restart the application services using **adstrtal.sh** script and verify the load balancer is distributing the connections.

## Configuring the Virtual IP (VIP) on ACE using ANM

The following procedure defines the VIP and its properties. A screen capture from the ANM is shown in Figure 14.

- **Step 1** Define a name for the VIP. In this example name is defined as APPHOST\_VIP.
- **Step 2** Assign an IP address to the VIP.
- **Step 3** Select the appropriate protocol. In this case, it's **tcp**.
- **Step 4** Assign the application protocol. In this case it's **https**.
- **Step 5** Assign the **Port** number. In this case, port **443** has been chosen.
- **Step 6** Assign the VLAN that the IP address defined in Step 2 belongs to.
- **Step 7** Assign the SLB and choose the pre-defined server farm.

#### Application Networking Manager 1.2 (0) Welcome admin Monitor Admin Tools Config >Devices >Load Balancing >Virtual Servers >Edit APPHOST\_VI Updating Virtual Server APPHOST\_VIP on Virtual Context 6K1:2:ORACLE Basic View -Properties \* VIP Name APPHOST\_VIP VIP IP: 101.1.5.50 \* Protocol: O any ⊙ tcp O udp \* Application Proto https 💽 Port: 443 \* VLAN: Available Items cted Items 200 -1133 1135 1105 🔺 + 7 SSI Termination Proxy Service Name: PROXY\_1 View Default L7 Load-Balancing Action 265995 Action \* Primary Action: loadbalance 💌 \* Server Farm:

#### Figure 14 Configuring the VIP on Cisco ACE

#### **Configuring Virtual IP (VIP) Using ACE CLI**

```
class-map match-all APPHOST_VIP
2 match virtual-address 101.1.5.50 tcp eq 443
policy-map multi-match VIPS
class APPHOST_VIP
   loadbalance vip inservice
   loadbalance policy APPHOST_POLICY
   loadbalance vip icmp-reply
   appl-parameter http advanced-options RE_USE
   ssl-proxy server PROXY_1
```

# **Configuring ACE for SSL**

This section of the document focuses on configuring the Cisco ACE for SSL. The document details how to configure parameter maps, SSL proxy services and class maps to build policy maps that determine the flow of information between the client, the ACE and the Oracle application hosts.

The following ACE to SSL configurations are provided:

- Configuring Parameter Maps Using ANM, page 15
- Configuring the SSL Key, page 17
- Importing the SSL Certificate, page 17
- Configuring SSL Proxy Services Using ANM, page 19

## **Configuring Parameter Maps Using ANM**

I

The following procedure is used for configuring a parameter map using ANM. Figure 15 shows an ANM screen involved in creating a parameter map.

- **Step 1** Define a name for the Parameter Map.
- **Step 2** Define the SSL Session Cache Timeout.
- Step 3 Select the Close Protocol Behavior (default is None).
- **Step 4** Select the SSL Version.

#### Figure 15 Creating a Parameter Map

Appress	onfig Monitor 🖓 Admin	wercome
Global Config > Devices	>SSL >Parameter Map	
arameter Map * Parameter Map Name: Queue Delay Timeout: Session Cache Timeout:	SSL_PARAM_1  3600 Reject evoked CPLs	
* Close Protocol Behavior: * SSL Version:	© None O Disabled C All O SSL3 © TLS1	
Parameter Map Cipher (1 Parameter Map Ciph	Row) er @ SSL_PARAM_1	
	Cipher Name	
1 C PSA WITH PC4	128 MD5	

265996

#### **Configuring Parameter Map Using ACE CLI**

parameter-map type ssl SSL\_PARAM\_1
 cipher RSA\_WITH\_RC4\_128\_MD5

For additional documentation on configuring parameter map, please refer to the following section of the configuration guide:

http://www.cisco.com/en/US/docs/interfaces\_modules/services\_modules/ace/v3.00\_A2/configuration/s sl/guide/initiate.html#wpmkr1075636

Digital certificates and key pairs are a form of digital identification for user authentication. CA's, such as VeriSign and Thawte, issue certificates that attest to the validity of the public keys they contain. A client or server certificate includes the following identification attributes:

- Name of the CA (the certificate issuer) and CA digital signature
- Serial number
- Name of the client or server (the certificate subject) that the certificate authenticates
- Subject's public key
- Time stamps that indicate the certificate's expiration date

A CA has one or more signing certificates that it uses for creating SSL certificates and certificate revocation lists (CRL). Each signing certificate has a matching private key that is used to create the CA signature. The CA makes the signing certificates (with the public key embedded) available to the public, enabling anyone to access and use the signing certificates to verify that an SSL certificate or CRL was actually signed by a specific CA.

The ACE requires certificates and corresponding key pairs for SSL termination.

The ACE acts as an SSL proxy server and terminates the SSL session between it and the client.

# **Configuring the SSL Key**

The following procedure is used for configuring a SSL Key. Figure 16 shows an ANM screen involved in creating the SSL Private Key.

- **Step 1** Define a name for the Private Key.
- **Step 2** Define the Private Key size (default is 1024)
- **Step 3** Enable the check box for "Exportable Key" if you would like the Private Key to be Exportable via ACE.

#### Figure 16 Creating a Private Key

	Application Networking Manager 1.2 (0)
y 🔍 Glo	obal O Tools
Confi	ig >Devices >SSL >Keys
Keys	
* 🔋 Name	e: kev1.pem
* Size:	1024
Type:	RSA
	☑ Exportable Key

265997

## **Importing the SSL Certificate**

You can import certificate and key pair files to the ACE from a remote secure server. To transfer these files, we recommend that you use a secure encrypted transport mechanism between the ACE and the remote server. The ACE supports the Secure Shell protocol (SSHv2), which provides secure encryption

communications between two hosts over an insecure network. The ACE supports file transport between network devices using Secure File Transfer Protocol (SFTP), File Transfer Protocol (FTP), and Trivial File Transfer Protocol (TFTP).

The following procedure is used for importing the SSL certificate. Figure 17 shows an ANM screen involved in importing the SSL Public Certificate.

- **Step 1** Define the protocol used to import the certificate
- **Step 2** Define the IP Address of the server where the certificate resides
- **Step 3** Define the Remote Filename of the certificate
- **Step 4** Define the Local Filename of the certificate
- **Step 5** Define the Username and Password
- **Step 6** Define a Passphrase used to access the certificate (Optional)
- **Step 7** Enable the check box for "Nonexportable" if you would like the Certificate to be nonexportable via ACE.

#### Figure 17 Creating a SSL Certificate

, ing oberne	ces>SSL>Certifi	ates				
ificates PName			Subject			
	Whttps://201.1.33. Import a Certificate,	39 - Import a Certi /Key file to a Devic	ificate/Key file to a D e	evice - Mozilla Firef	ох 🛋	
	* Protocol:	SFTP 🔽				
	* IP Address:					
	* Local Filename:					
	* Username:					
	* Password:		Confirm:			
	Passphrase:		Confirm:			
	1	Nonexportable				

#### Importing the SSL Certificate Using CLI

crypto import sftp IP\_ADDRESS Passphrase

crypto import sftp 1.1.1.1 Username Password Localfile

For additional documentation on configuring Keys and Certificates please refer to the following section of the configuration guide:

 $http://www.cisco.com/en/US/docs/interfaces_modules/services_modules/ace/v3.00_A1/configuration/s_sl/guide/certkeys.html$ 

# **Configuring SSL Proxy Services Using ANM**

The following procedure is used for configuring SSL proxy services using ANM. Figure 18 shows an ANM screen involved in configuring SSL proxy services on the Cisco ACE.

- **Step 1** Select the pre-defined SSL Proxy Service Name.
- **Step 2** Select the pre-defined SSL private key.
- **Step 3** (Optional) Select the SSL Chain Group.
- **Step 4** (Optional) Select the SSL Auth Group.
- **Step 5** Select the pre-defined SSL public certificate.
- **Step 6** Select the pre-defined SSL Parameter Map Name.

#### Figure 18 Configuring SSL Proxy Services

Applica	tion Networking Manager 1.2 (0)	
- <mark></mark>	Config 🦗 Monitor 🕞 Admin	
oy 🤜 Global 🙁 Tools	AL	
Config >Devices	>SSL>Proxy Service	
Proxy Service		
* 💡 Proxy Service Name:	PROXY_1	
+ Key List:	C N/A © key1.pem	
Certificate List:	○ N/A ⓒ cert1.pem	
🛃 Chain Group Name:	• N/A	
Auth Group Name:	• N/A	
Parameter Map Name:	C N/A @ SSL_PARAM_1	

265999

#### **Configure SSL Proxy Services Using CLI**

I

```
parameter-map type ssl SSL_PARAM_1
  cipher RSA_WITH_RC4_128_MD5
!
ssl-proxy service PROXY_1
  key key1.pem
  cert cert1.pem
  ssl advanced-options SSL_PARAM_1
```

For additional documentation on configuring SSL proxy services please refer to the following section of the configuration guide:

 $http://www.cisco.com/en/US/docs/interfaces_modules/services_modules/ace/v3.00_A2/configuration/s\ lb/guide/classlb.html#wpmkr1076742$ 

# References

The following Oracle and Cisco reference material is available.

#### **Oracle Reference Documents**

1. Using Autoconfig to Manage system configurations with Oracle Applications 11i (Metalink Noteid 165195.1)

 $http://metalink.oracle.com/metalink/plsql/ml2_documents.showFrameDocument?p_database_id=NOT\&p_id=165195.1$ 

**2.** Advanced Configurations and Topologies for Enterprise Deployments of E-business Suite 11i (Metalink Noteid 217368.1)

 $http://metalink.oracle.com/metalink/plsql/ml2_documents.showFrameDocument?p_database_id=NOT\&p_id=217368.1$ 

#### **Cisco Reference Documents**

1. Cisco Application Control Engine Configuration Guide:

 $http://www.cisco.com/en/US/docs/interfaces_modules/services_modules/ace/v3.00\_A1/configuration/administration/guide/admgd.html$ 

CCSP, the Cisco Square Bridge logo, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0406R)

Copyright © 2008, Cisco Systems, Inc. All rights reserved.

ſ