radware

TESTING & INTEGRATION GROUP

AppDirector and AppXcel With Oracle Application Server 10g Release 3 (10.1.3.1.0) - Oracle SOA Suite Enterprise Deployment

TECHNICAL DOCUMENT
Test Engineer: Iztok Umek
AUTHOR: Chris Hensel
DATE: Wednesday, July 16, 2008
Version: 2.0

Introduction

AppDirector and AppXcel within the Oracle SOA Suite

Oracle's SOA Suite is a complete set of service infrastructure components for building, deploying, and managing SOAs. Oracle SOA Suite enables services to be created, managed and orchestrated into composite applications and business processes. Architects and developers are addressing the complexity of their application and IT environments with Oracle SOA Suite which facilitates the development of enterprise applications as modular business services that can be easily integrated and reused, creating a truly flexible, adaptable IT infrastructure.

With AppDirector and AppXcel, the Oracle SOA Suite can be further enhanced to provide increased scalability, performance and reliability to the benefits offered by the Oracle SOA Suite. This document describes the architecture and configuration detail to integrate the Radware products into the SOA environment

Software and Hardware used

Radware's AppDirector 1000, software version 1.03.04

Radware's AppXcel 4000, software version 1.02.06

Solution Details

The solution described below employs an AppDirector for load balancing incoming application service requests to the Oracle SOA application, session persistency, and web acceleration configured with an AppXcel farm for SSL decryption/encryption off loading. The AppDirector is configured with 5 server farms: HTTP and HTTPS SSO farms, HTTP and HTTPS SOA farms, and an Oracle Internet Directory farm. These entities are described below. The AppXcel is configured with two tunnels. Configuration details for both the AppDirector and AppXcel are given later in the document.

The diagram below shows a schematic view of the environment under test, indicating the flows between the Oracle SOA Suite components and the Radware AppDirectors and AppXcels.

Schematic View of Test Environment

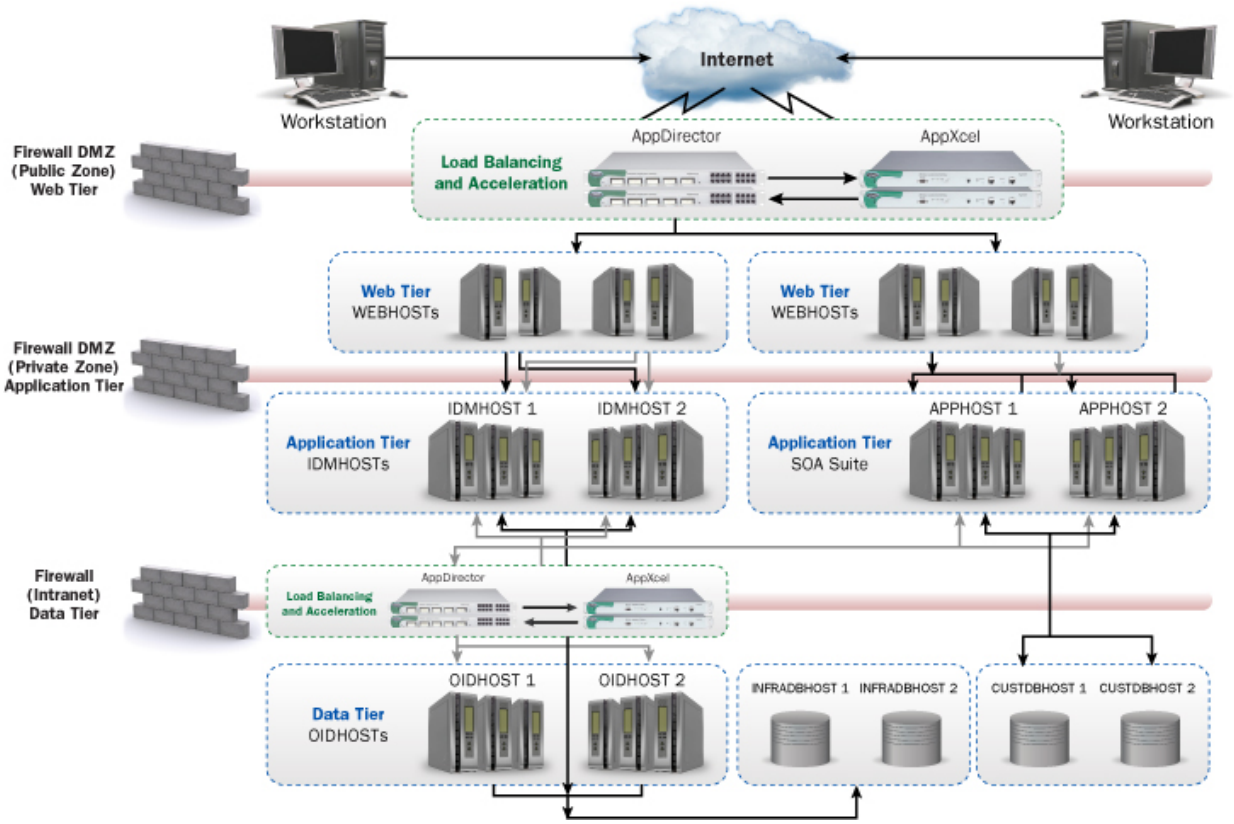


Diagram 1.0 - Logical Topology

How it works

A user desiring access to an SOA application generates a request directed toward the Oracle HTTP Server (OHS). The AppDirector load balances these requests between the defined Oracle HTTP Servers. In the tested scenario, the SOA application is registered with Oracle Containers for Java (OC4J) as a Single Sign-On application. So when the OHS server receives the request the SSO process checks whether or not a cookie exists for the user which would indicate that it has already been authenticated. If not, the OHS redirects the user to an SSO process login / password prompt and the user then enters login credentials. This connection is secure and when the response reaches the AppDirector it is forwarded to the AppXcel farm to be decrypted and processed.

Also for the test, the SOA application is defined to the Oracle Internet Directory for identity management so the SSO process queries the OID server using the LDAP protocol for the user's Distinguished Name (DN) and to obtain role / group information for user access permissions. This request is passed through the AppDirector where it is load balanced across the OID server farm. Once the user credentials are authenticated the application binds to the directory and the user's group / role information is retrieved from the OID. Subsequent requests by the user to the SOA application are then passed directly to the SOA application server and load balanced appropriately.

AppDirector - Policies, Farms, Servers

There are 3 VIPs defined on the AppDirector with 2 policies defined for each VIP. The first VIP (10.143.181.37) has 2 policies associated with it: policy **oidtcp389** and policy **oidtcp636.** These policies listen for inbound traffic on TCP ports 389 and 636 directed toward the Oracle Information Directory servers.

Policy: oidtcp389
Port: TCP port 389
Farm: oid
Servers:
Lnxi02 – 10.143.180.247
Lnxi03 – 10.143.180.248

Policy: oidtcp636
Port: TCP port 636
Farm: oid
Servers:
Lnxi02 – 10.143.180.247
Lnxi03 – 10.143.180.248

The second VIP (10.143.181.38) has 2 policies associated with it. The policy **soahttp** listens for inbound HTTP traffic directed toward the Oracle Application Servers and sends matching traffic to the servers associated with the SOA farm. The policy **soahttps** listens for inbound HTTPS traffic and passes it to the AppXcel farms to offload the SSL processing.

Policy: soahttps
Port: TCP port 443
Farm: soassl
Servers:

Tunnel_192. 168. 1.101
Tunnel_192. 168. 1.201

Policy: soahttp
Port: TCP port 80
Farm: soahttp
Servers:

Lnxi06 – 10.143.180.251:7777
Lnxi07 – 10.143.180.252:7777

The third VIP (10.143.181.36) has 2 policies associated with it: policy **ssohttp** listens for inbound HTTP traffic directed toward the SSO service from from OHS, and **ssohttps** which listens for HTTPS traffic and directs the matching inbound traffic to the AppXcel EP Farm to off load the SSL processing.

Policy: ssohttp
Port: TCP port 80
Farm: sso
Servers:

Lnxi02: 10.143.180.247:7777
Lnxi03: 10.143.180.248:7777

Policy: ssohttps
Port: TCP port 443
Farm: ssohttps
Servers:

Tunnel_192. 168. 1.102
Tunnel_192. 168. 1.202

Health Monitoring

The AppDirector constantly monitors the health of the three server types, OID, SSO and SOA using LDAP and HTTP Get methods requests. When a server is detected to be down, based upon application responses, the AppDirector automatically switches to other available servers.

The OID Health Check uses a Method of LDAP with the following Method Arguments:

User Name:	cn=cladmin
Password:	(cladmin password)
Attribute name:	cn
Search value:	asdb
Dest Port:	389

The SSO Health Check uses a Method of HTTP with the following Method Arguments:

Path:	/sso/status
HTTP method:	GET
Proxy HTTP:	Yes
Pragma Nocache:	Yes
Match Search String:	OC4J_Security is running. Match Mode: String Exists
Dest Port:	7777

The SOA Health Check uses a Method of HTTP with the following Method Arguments:

Path:	/
HTTP method:	GET
Proxy HTTP:	Yes
Pragma Nocache:	Yes
HTTP Return Code:	200
Dest Port:	7777

AppXcel – Tunnels

The AppXcel is being used to accelerate SSL traffic. It handles the SSL key negotiation with the client and encrypting and decrypting of the communication with it. The AppXcel uses a specialized hardware for that, and can handle a large amount of concurrent users.

There are 4 tunnels defined on the AppXcel:

Virtual Host IP	Remote IP	Listen Port	Remote Port
192.168.1.101	10.143.181.38	443	80
192.168.1.102	10.143.181.36	443	80
1921.68.1.201	10.143.181.38	443	80
192.168.1.202	10.143.181.36	443	80

Network Diagram

mySOAcompany with Oracle Single Sign-On

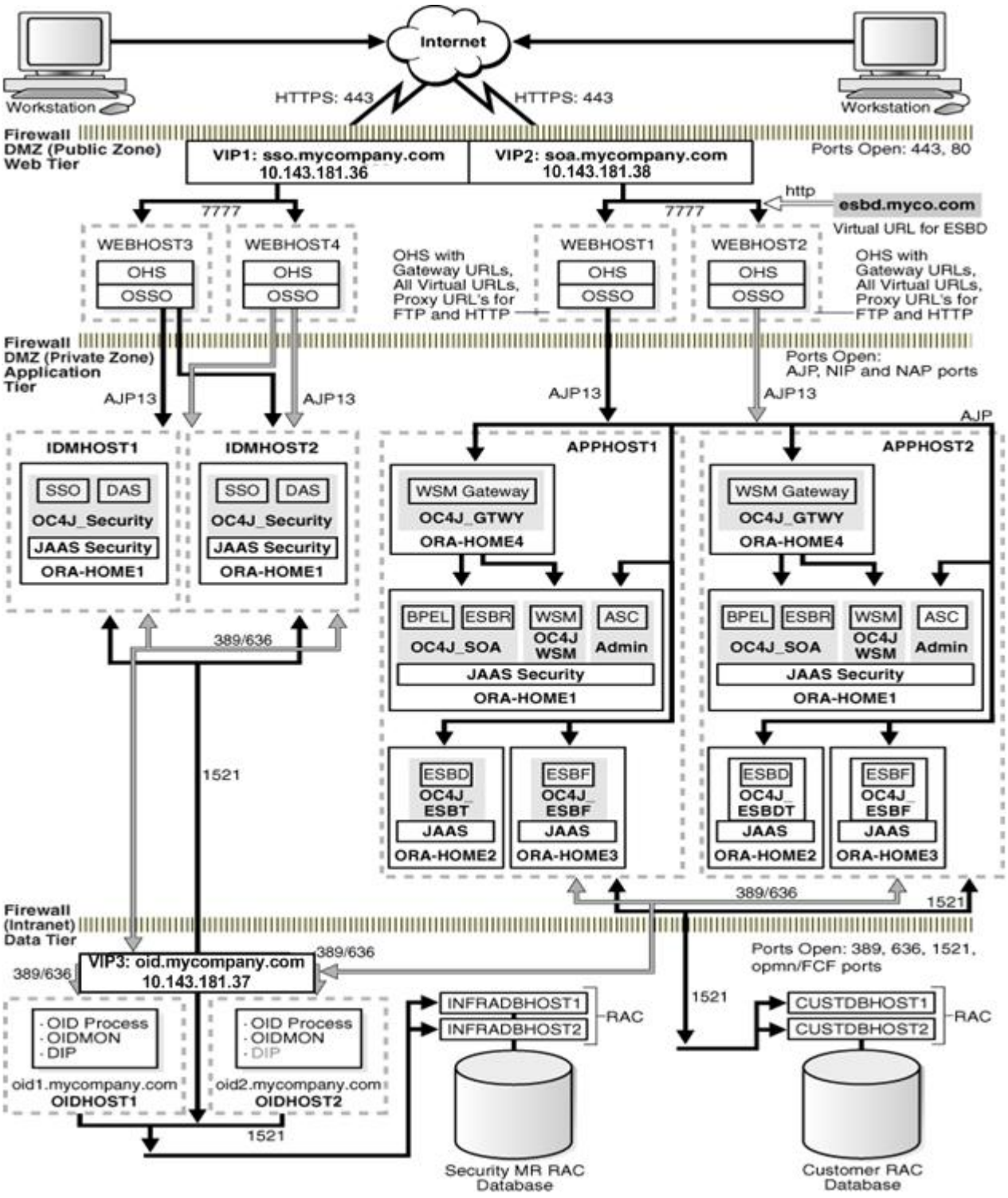


Diagram 2.0 - Physical Topology

Configuration

Create Interfaces with the following attributes:
To configure, reference Appendix 1 - Initial AppDirector Configuration – step3

Create IP 10.143.180.215/24 on port 2
Create IP 192.168.1.1/24 on port 1

Create farms with the following attributes:
To configure, reference Appendix 1 - Farm Configuration – step3

Farm Name:	oid
Aging Time:	300
Dispatch Method:	Cyclic
Sessions Mode:	EntryPerSession
Connectivity Check:	No Checks

Farm Name:	sso
Aging Time:	600
Dispatch Method:	Cyclic
Sessions Mode:	EntryPerSession
Connectivity Check:	No Checks

Farm Name:	ssossl
Aging Time:	300
Dispatch Method:	Cyclic
Sessions Mode:	EntryPerSession
Connectivity Check:	TCP Port
Connectivity Check Port:	HTTPS

Farm Name:	soa
Aging Time:	600
Dispatch Method:	Cyclic
Sessions Mode:	EntryPerSession
Connectivity Check:	No Checks

Farm Name:	soassl
Aging Time:	600
Dispatch Method:	Cyclic
Sessions Mode:	EntryPerSession
Connectivity Check:	TCP Port
Connectivity Check Port:	HTTPS

Create servers with the following attributes:
To configure, reference Appendix 1- Adding Servers to the Farm – step3

Farm Name:	oid
Server Address:	10.143.180.247
Server Port:	None
Server Name:	lnxi02
Client NAT:	Enabled
Client NAT Range:	10.143.181.39

Farm Name:	oid
Server Address:	10.143.180.248
Server Port:	None
Server Name:	lnxi03

Client NAT:	Enabled
Client NAT Range:	10.143.181.39
Farm Name:	ssossl
Server Address:	192.168.1.102
Server Port:	443
Server Name:	Tunnel_192.168.1.102
Farm Name:	ssossl
Server Address:	192.168.1.202
Server Port:	443
Server Name:	Tunnel_192.168.1.202
Farm Name:	sso
Server Address:	10.143.180.247
Server Port:	7777
Server Name:	lnxi02
Client NAT:	Enabled
Client NAT Range:	10.143.181.39
Farm Name:	sso
Server Address:	10.143.180.248
Server Port:	7777
Server Name:	lnxi03
Client NAT:	Enabled
Client NAT Range:	10.143.181.39
Farm Name:	soassl
Server Address:	192.168.1.101
Server Port:	443
Server Name:	Tunnel_192.168.1.101
Farm Name:	soassl
Server Address:	192.168.1.201
Server Port:	443
Server Name:	Tunnel_192.168.1.201
Farm Name:	soa
Server Address:	10.143.180.251
Server Port:	7777
Server Name:	lnxi06
Client NAT:	Enabled
Client NAT Range:	10.143.181.39
Farm Name:	soa
Server Address:	10.143.180.252
Server Port:	7777
Server Name:	lnxi07
Client NAT:	Enabled
Client NAT Range:	10.143.181.39

Create L4 Policies with the following attributes:
To configure, reference Appendix 1- Layer 4 Policy Configuration – step3

Virtual IP:	10.143.181.37
L4 Protocol:	TCP

L4 Port:	389
L4 Policy Name:	oidtcp389
Farm Name:	oid
Application:	TCP

Virtual IP:	10.143.181.37
L4 Protocol:	TCP
L4 Port:	636
L4 Policy Name:	oidtcp636
Farm Name:	oid
Application:	TCP

Virtual IP:	10.143.181.36
L4 Protocol:	TCP
L4 Port:	80
L4 Policy Name:	ssohttp
Farm Name:	sso
Application:	HTTP

Virtual IP:	10.143.181.36
L4 Protocol:	TCP
L4 Port:	443
L4 Policy Name:	ssohttps
Farm Name:	ssossl
Application:	HTTPS

Virtual IP:	10.143.181.38
L4 Protocol:	TCP
L4 Port:	80
L4 Policy Name:	soahttp
Farm Name:	soa
Application:	HTTP

Virtual IP:	10.143.181.38
L4 Protocol:	TCP
L4 Port:	443
L4 Policy Name:	soahttps
Farm Name:	soassl
Application:	HTTPS

Create Health Checks with the following attributes:
To configure, reference Appendix 1 - Health Monitoring Configuration – step7

Health Check:	OID-lnxi02
Check Element:	lnxi02
Method:	LDAP
Method Arguments:	
User Name:	cn=cladmin
Password:	(cladmin password)
Attribute name:	cn
Search value:	asdb
Dest Port:	389

Health Check:	OID-lnxi03
Check Element:	lnxi03
Method:	LDAP

Method Arguments:	
User Name:	cn=cladmin
Password:	(cladmin password)
Attribute name:	cn
Search value:	asdb
Dest Port:	389
Health Check:	SSO-HealthCheck-lnxi02
Check Element:	lnxi02
Method:	HTTP
Method Arguments:	
Path:	/sso/status
HTTP method:	GET
Proxy HTTP:	Yes
Pragma Nocache:	Yes
Match Search String:	OC4J_Security is running.
Match Mode:	String Exists
Dest Port:	7777
Health Check:	SSO-HealthCheck-lnxi03
Check Element:	lnxi03
Method:	HTTP
Method Arguments:	
Path:	/sso/status
HTTP method:	GET
Proxy HTTP:	Yes
Pragma Nocache:	Yes
Match Search String:	OC4J_Security is running.
Match Mode:	String Exists
Dest Port:	7777
Health Check:	SOA-lnxi06
Check Element:	lnxi06
Method:	HTTP
Method Arguments:	
Path:	/
HTTP method:	GET
Proxy HTTP:	Yes
Pragma Nocache:	Yes
HTTP Return Code:	200
Dest Port:	7777
Health Check:	SOA-lnxi07
Check Element:	lnxi07
Method:	HTTP
Method Arguments:	
Path:	/
HTTP method:	GET
Proxy HTTP:	Yes
Pragma Nocache:	Yes
HTTP Return Code:	200
Dest Port:	7777

Appendix 1: Step by step AppDirector configuration

Overview

This appendix details the step by step AppDirector configuration via the Web Based Management GUI. The IP addresses and names are examples and should be replaced with ones that reflect your network configuration.

The following steps should be done in order due to configuration dependencies, e.g. a Farm has to be created before Servers can be added to it. If desired parameters are not found, then either a required configuration step was not first performed or the page has to be refreshed.

Initial AppDirector Configuration

Using a serial cable and a terminal emulation program, connect to the AppDirector. The default console port settings are:

- Bits per Second: 19200
- Data Bits: 8
- Parity: None
- Stop Bits: 1
- Flow Control: None

1. Using a browser, connect to the management IP Address of the AppDirector (192.168.1.1) via HTTP or HTTPS. The default username and password are “radware” and “radware”.

2. Using the following Command line, Assign the following management IP address to interface 1 of the AppDirector (Dedicated Management Interface): 192.168.1.1 / 24

```
net ip-interface create 192.168.1.1 255.255.255.0 1
```

3. Create a default gateway route entry on the AppDirector pointing to 192.168.1.254.

```
net route table create 0.0.0.0 0.0.0.0 192.168.1.254 -i 1
```

Failure to establish a connection may be due to the following:

- Incorrect IP Address in the browser
- Incorrect IP Address or default route configuration in the AppDirector
- Failure to enable Web Based Management or Secure Web Based Management in the AppDirector
- If the AppDirector can be successfully pinged, attempt to connect to it via Telnet or SSH. If the pinging or the Telnet/SSH connection are unsuccessful, reconnect to the AppDirector via its console port. Once connected, verify and correct the AppDirector’s configuration as needed.

Note: Items circled in red indicate settings that need to be entered or changed. Items not circled should be left to default settings.

Web Interface Examples

Farm Configuration

1. From the menu, select **AppDirector ⇨ Farms ⇨ Farm Table** to display the **Farm Table** page

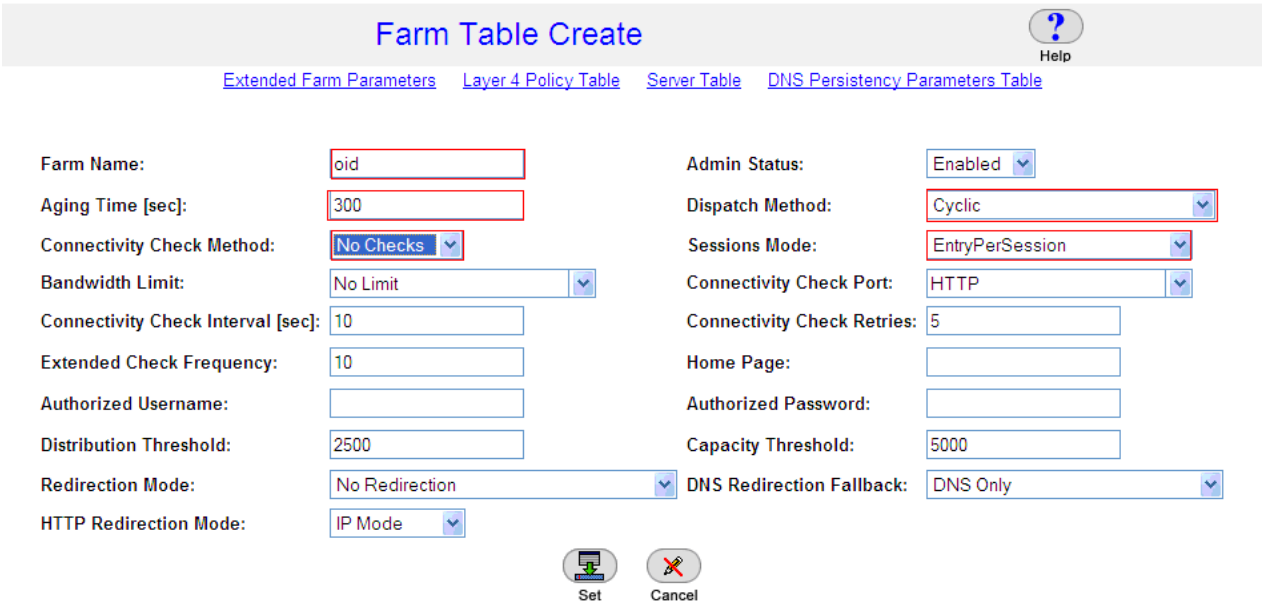
2. Click the Create button.
3. On the **Farm Table Create** page, enter the necessary parameters as shown below

Create farm with the following attributes:

- Farm Name: oid
- Aging Time: 300
- Dispatch Method: Cyclic
- Sessions Mode: EntryPerSession
- Connectivity Check: No Checks

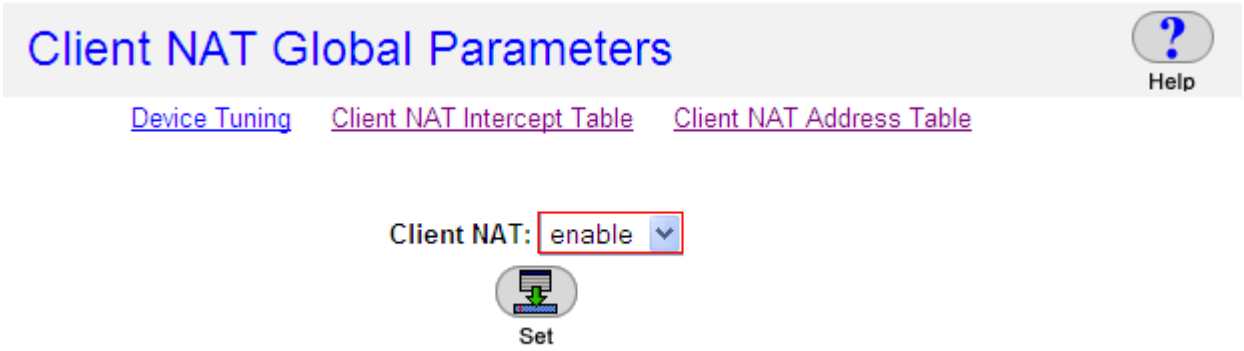
Note: The **Aging Time** value is based on the application and should be set for a few seconds longer then the application timeout.

4. Click the **Set** button to save parameters.



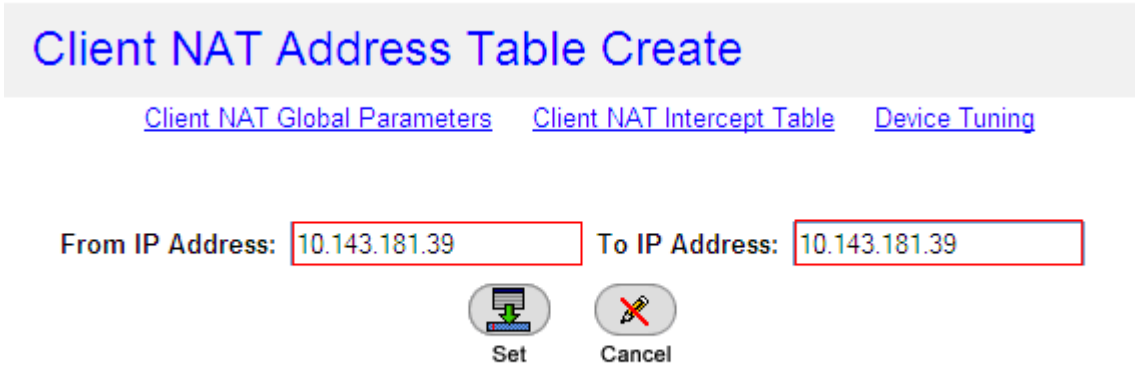
Client NAT Configuration

1. From the menu, select **AppDirector ⇨ NAT ⇨ Client NAT** to display the **Global Parameters** page.
2. On the **Global Parameters** page, change the parameters as shown below:

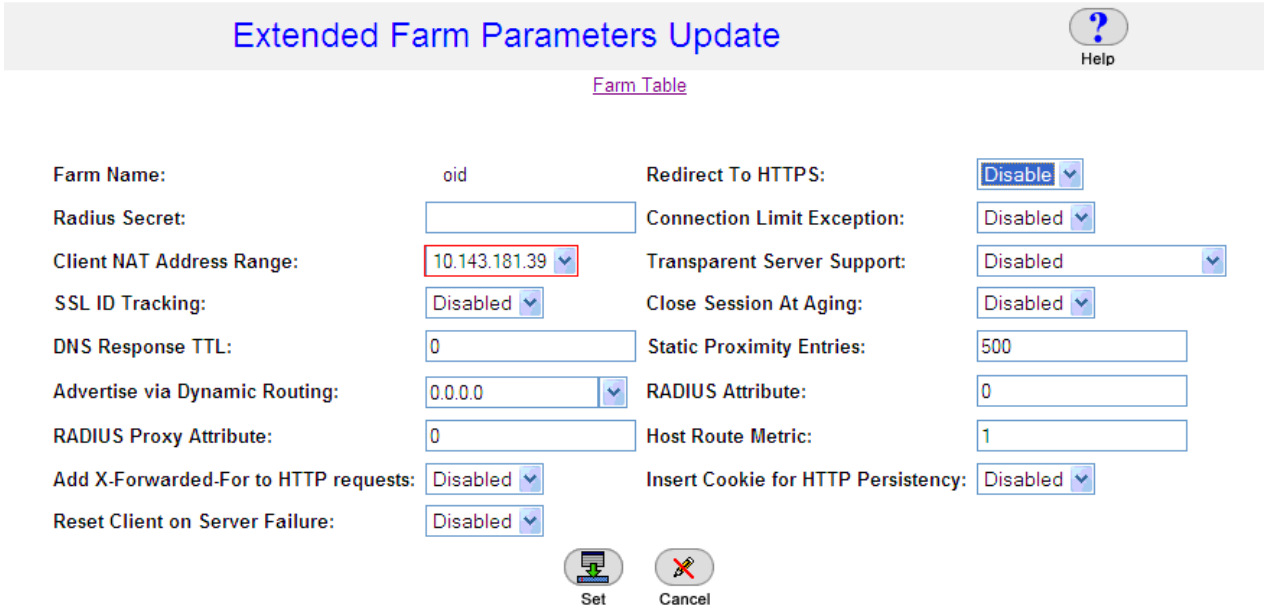


3. Click the **Set** button to save parameters.
4. Click the **Client NAT Intercept Table** hyperlink at the top of the configuration window.
5. Click the **Create** button.
6. On the **Client NAT Intercept Table Create** page, enter the necessary parameters as shown below.

7. Click the **Set** button to save parameters.
8. Click the **Client NAT Address Table** hyperlink at the top of the configuration window.
9. Click the **Create** button.
10. On the **Client NAT Address Table Create** page, enter the necessary parameters as shown below.

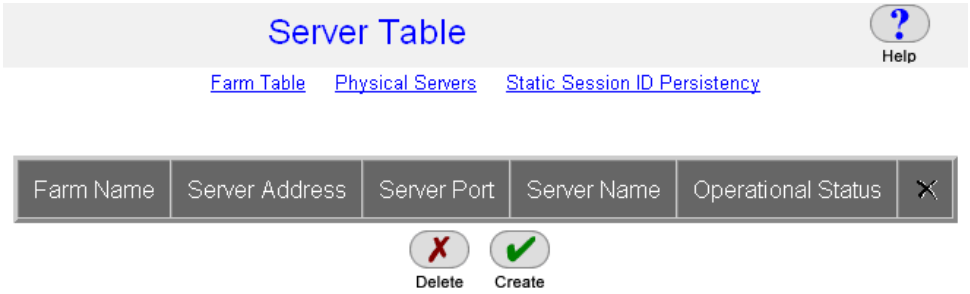


11. Click the **Set** button to save parameters.
12. From the menu, select **AppDirector ⇨ Farms ⇨ Farm Table** to display the **Farm Table.**
13. Click the **Extended Farm Parameter** hyperlink near the top of the page.
14. On the **Extended Farm Parameter** page, enter the necessary parameters as shown below:
15. Click the **Set** button to save parameters



Adding Servers to the Farm

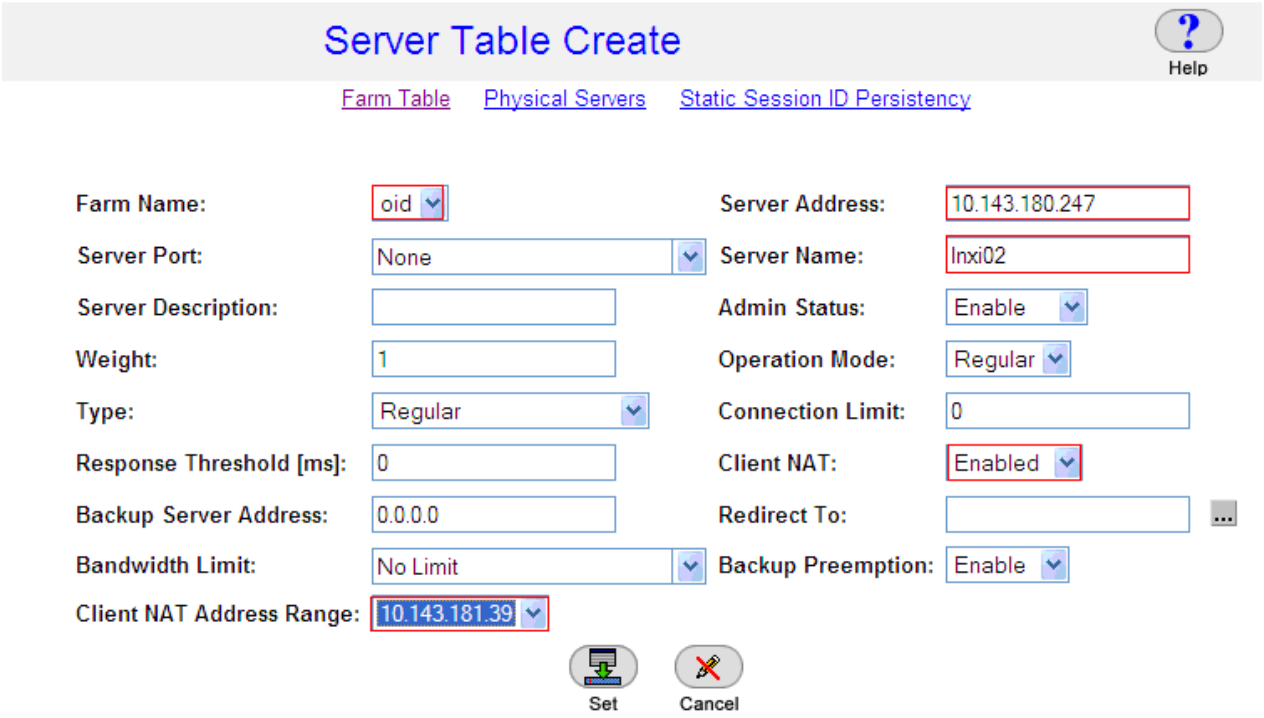
1. From the menu, select **AppDirector ⇨ Servers ⇨ Application Servers** to display the **Server Table** page similar to the one shown below:



2. Click the **Create** button.
3. On the **Server Table Create** page, enter the necessary parameters as shown below:

Create servers with the following attributes:

Farm Name:	oid
Server Address:	10.143.180.247
Server Port:	None
Server Name:	lnxi02
Client NAT:	Enabled
Client NAT Range:	10.143.181.39



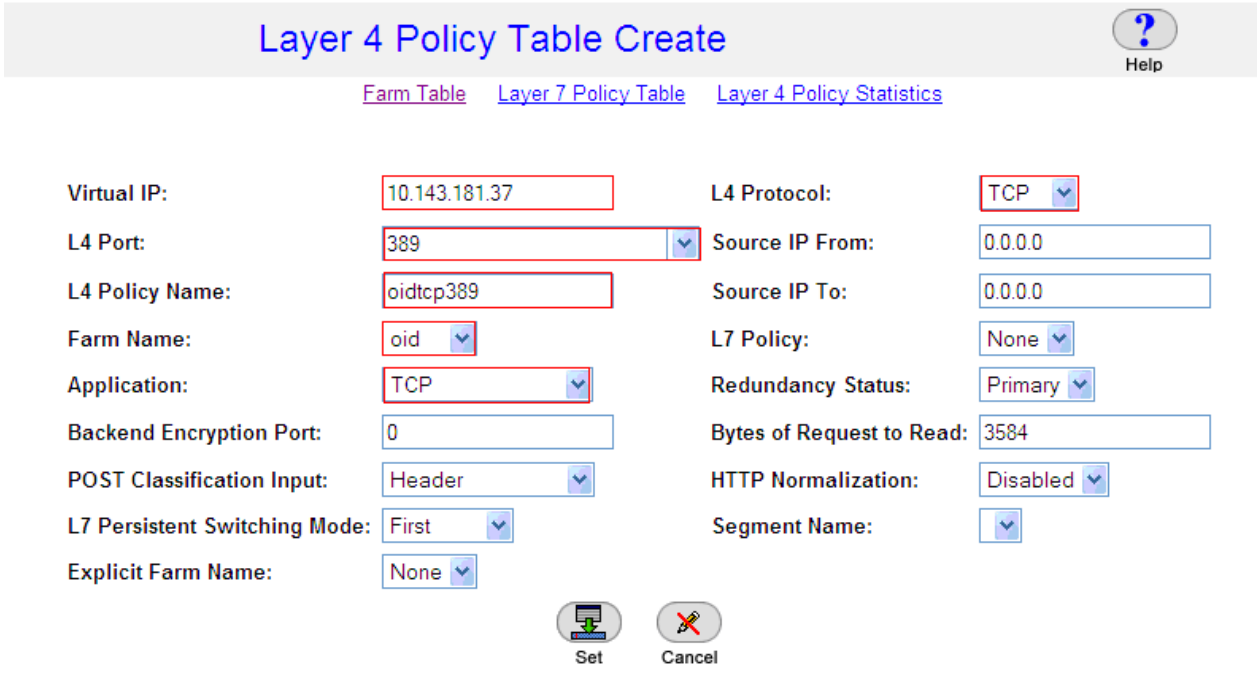
Layer 4 Policy Configuration

1. From the menu, select **AppDirector ⇨ Layer 4 Farm Selection ⇨ Layer 4 Policy** Table to display the **Layer 4 Policy Table** page similar to the one shown below:

2. Click the **Create** button.
3. On the **Layer 4 Policy Table Create** page, enter the necessary parameters as shown below.
4. Click the **Set** button to save the parameters.

Create L4 Policies with the following attributes:

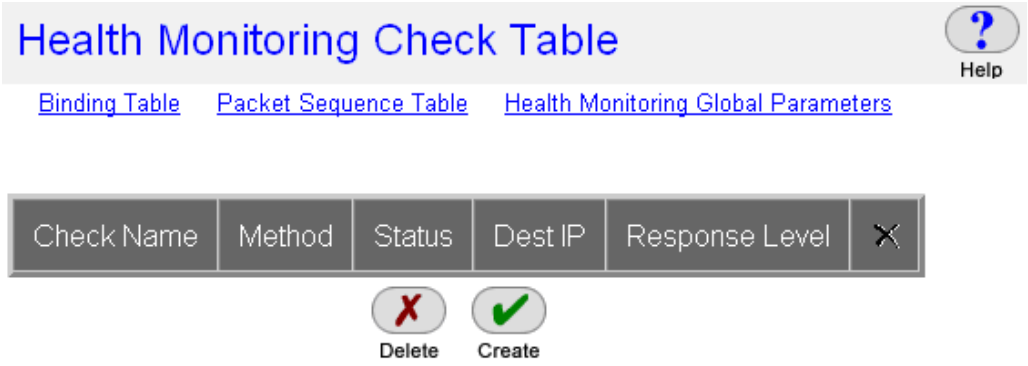
Virtual IP:	10.143.181.37
L4 Protocol:	TCP
L4 Port:	389
L4 Policy Name:	oidtcp389
Farm Name:	oid
Application:	TCP



Health Monitoring Configuration

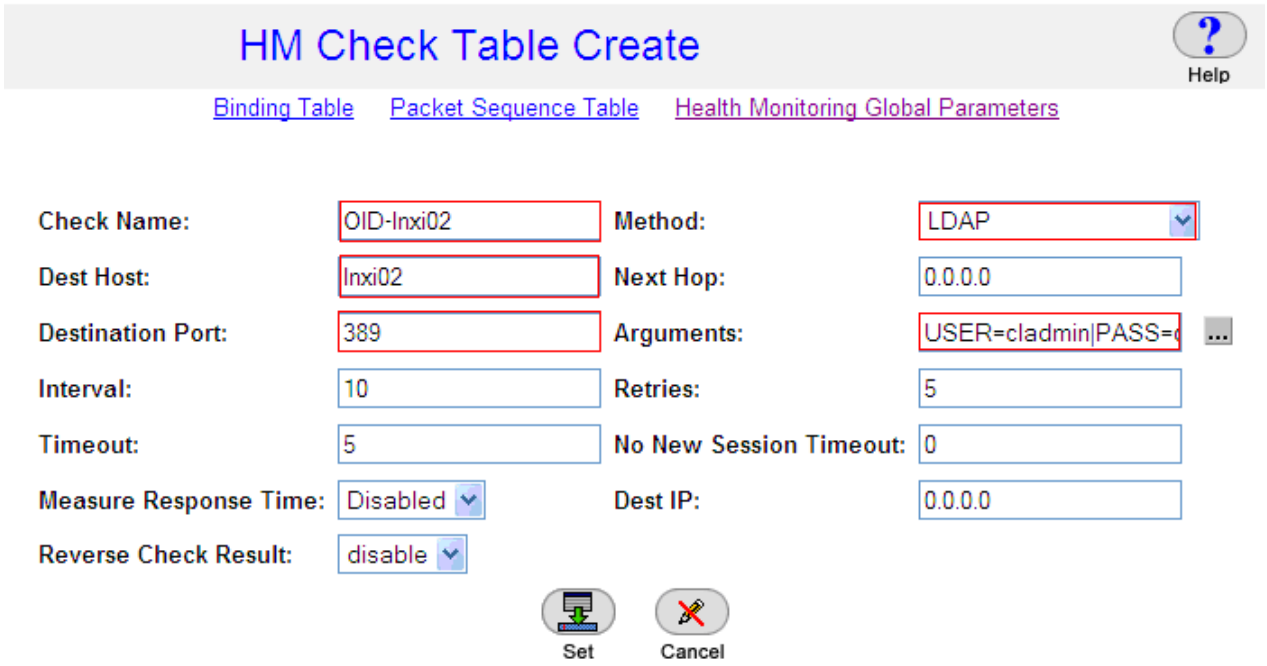
1. From the menu, select **Health Monitoring ⇨ Global Parameters** to display the **Health Monitoring Global Parameters** page.
2. On the **Health Monitoring Global Parameters** page, change the parameters as shown below:

3. Click the **Set** button to save the parameters.
4. Create the Health Monitoring Check for the Server.
5. From the menu, select **Health Monitoring ⇨ Check Table** to display the **Health Monitoring Check Table** page similar to the one shown below:

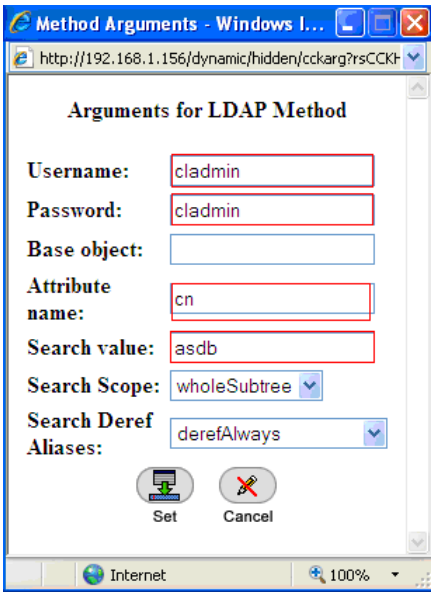


6. Click the **Create** button.
7. On the HM Check Table Create page, enter the necessary parameters as shown below:

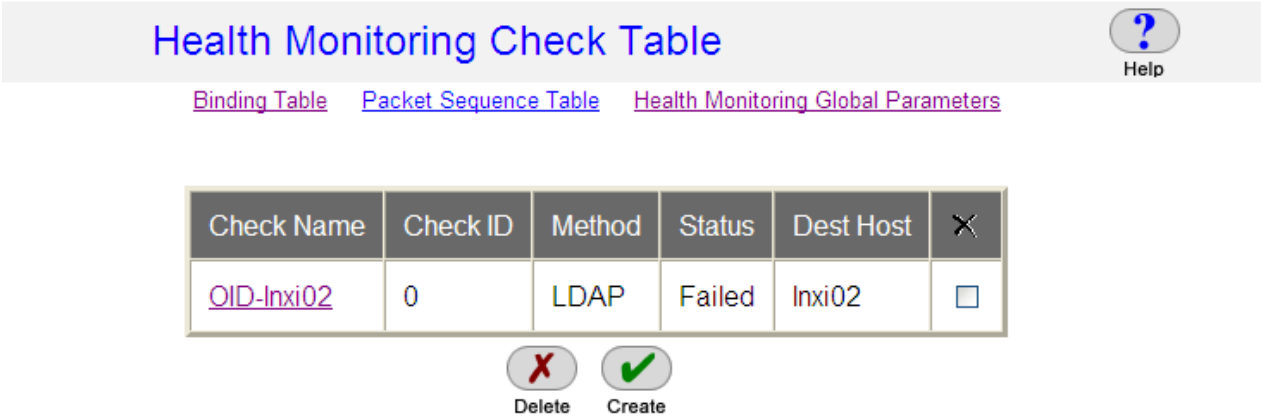
Health Check:	OID-lnxi02
Check Element:	lnxi02
Method:	LDAP
Method Arguments:	
User Name:	cn=cladmin
Password:	(*cladmin password*)
Attribute name:	cn
Search value:	asdb
Dest Port:	389



8. Before clicking the Set button, choose the button next to Arguments ... to populate the specific settings for the rest of this check.
9. Enter the information below:

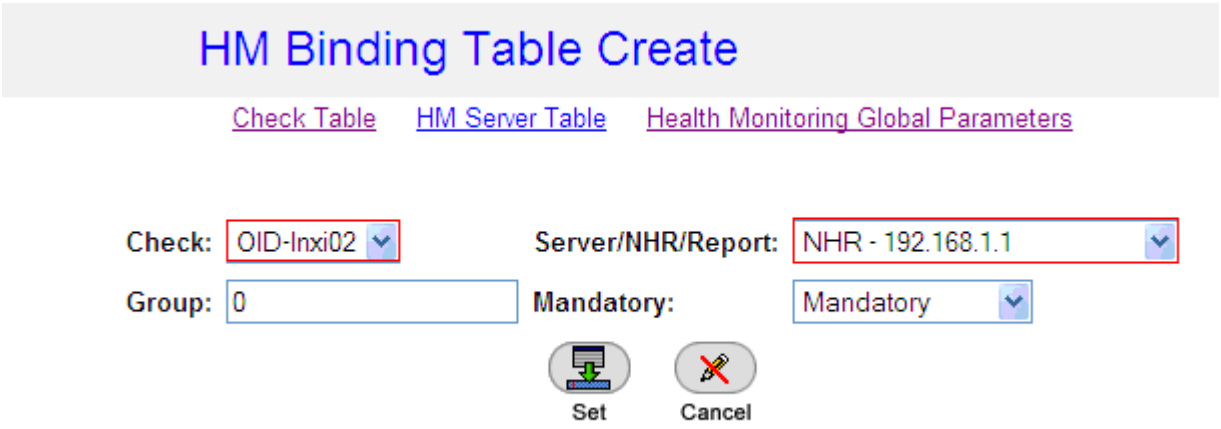


10. Click the Set button for the Method Arguments and click the Set button again in the HM Check Table Create window.
11. Verify that the new entry was created on the **Health Monitoring Check Table** page:

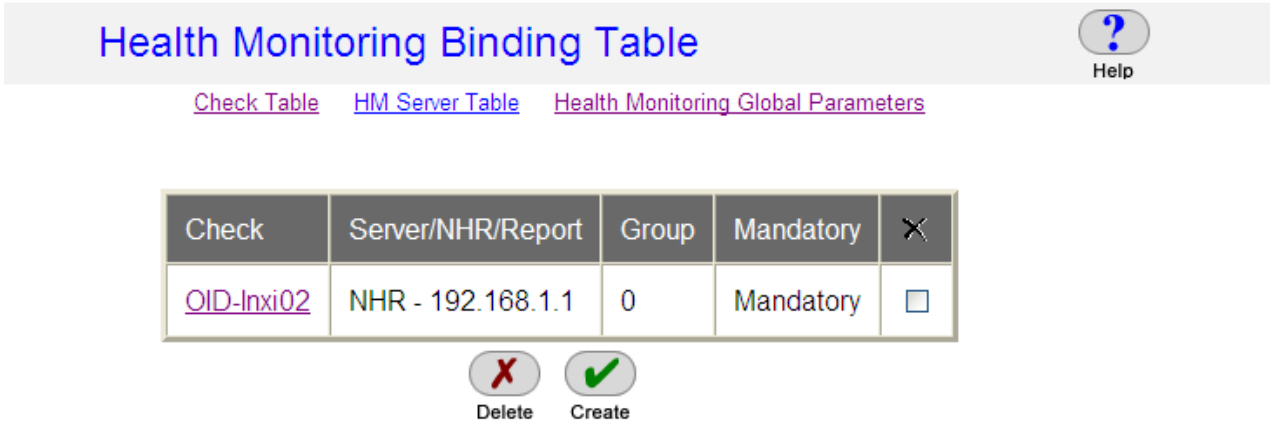


12. Create the Health Monitoring Binding for the Server
13. From the menu, select **Health Monitoring ⇨ Binding Table** to display the **Health Monitoring Binding Table** page similar to the one shown below:

14. Click the **Create** button.
15. On the **HM Binding Table Create** page, enter the necessary parameters as shown below:



16. Click the **Set** button to save parameters.
17. Verify that the new entry was created on the **Health Monitoring Table** page



Initial AppXcel Configuration

1. Using a serial cable and a terminal emulation program, connect to the AppDirector. The default console port settings are:

   - Bits per Second: 19200
   - Data Bits: 8
   - Parity: None
   - Stop Bits: 1
   - Flow Control: None

2. Using a browser, connect to the management IP Address of the AppDirector (192.168.1.1) via **HTTPS**. The default username and password are “radware” and “radware”.

3. Assign a management address to LAN1:

   net management-ip create 192.168.1.2 255.255.255.0 -inf 1

4. Assign a default Gateway

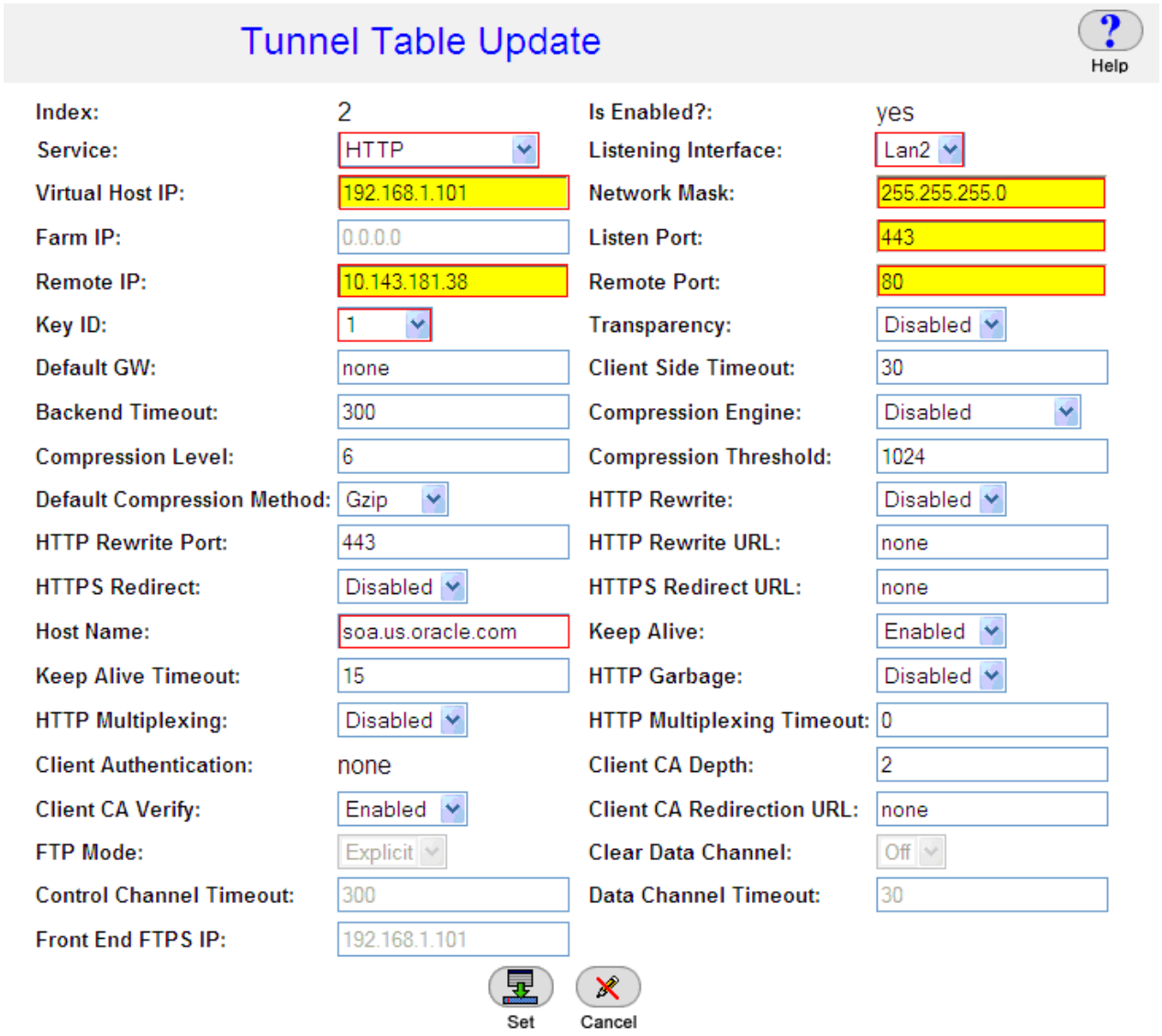
   net route table create default-gw 192.168.1.10

Tunnel creation

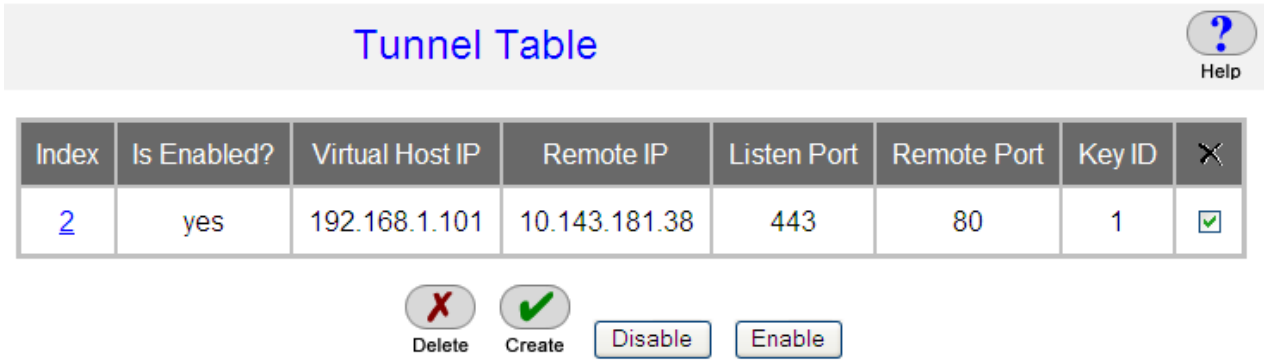
1. From the menu, select **Tunnel ⇨Table** to display the **Tunnel Table** page
2. On the **Tunnel Table** page, enter the necessary parameters as shown below:

Web Interface AppXcel Tunnel example

```
Enabled                       : yes
LAN                           : 2
Default Gateway               : 192.168.1.10
Virtual Host IP               : 192.168.1.101
Listening Port                : 443
Interface IP                  : 192.168.1.101
Netmask                       : 255.255.255.0
Remote IP                     : 10.143.181.38
Remote Port                   : 80
Transparent                   : on
Hostname                      : soa.us.oracle.com
Keep Alive                    : on
Keep Alive Timeout            : 15
Compression method            : gzip
Gzip engine                   : off
HTTP redirect                 : off
HTTP redirect port            :
HTTPS redirect                : off
HTTP multiplexing             : off
HTTP multiplexing timeout : 0
HTTP garbage                  : off
SSL Key ID                    : 1
CipherSuites                  : RSA
Backend SSL                   : off
Backend CipherSuites          : LOW
Backend L7 LB port            : 0
Service                       : http
Client CA                     : no
CRL                           : no
Client Timeout                : 30
Backend Timeout               : 300
Cache status                  : off
Cache expiration time         : 86400
Jpeg reduction status         : off
Jpeg reduction ratio          : 50
Url-Rewerite Policy           : none
  Url-Rewrite mode            : disable
Url-Rewrite Default           : none
URL LDAP authentication       : off
Cdp tunnel bindings           : none
```



3. Click the Set button to save parameters.
4. Verify that the new entry was created on the Table page.



Appendix 2: AppXcel – TLS Key and Certificate Details

TLS Key Table

appxcel key table get Keys:

Index	Size	Cert	Common Name
1	1024	Crt	soa.us.oracle.com
2	1024	Crt	sso.us.oracle.com

Certificate Details

```
Certificate (csr/crt/int)                          = crt
Date not before                                    = Apr 17 19:09:05 2007 GMT
Date not after                                     = Apr 16 19:09:05 2008 GMT
Key Size (512/1024/2048)                           = 1024
Common Name                                        = soa.us.oracle.com

Tunnel IP / Server Name                            1 soa.us.oracle.com
```

Note: This Certificate is also bound to “Key Index 2” as well.

Appendix 3: Radware Technical Support

Radware offers technical support for all of its products through the Radware Certainty Support Program. Please refer to your Certainty Support contract, or the Radware Certainty Support Guide available at:

http://www.radware.com/content/support/supportprogram/default.asp.

For more information, please contact your Radware Sales representative or:

U.S. and Americas: (866) 234-5763

International: +972(3) 766-8666