

Radware's AppDirector and Oracle Siebel Customer Relationship Management (CRM) 8.0 Implementation Guide

Products:

Radware AppDirector Software: AppDirector version 2.00.01 Platform: On-Demand Switch II XL

Oracle Siebel 8

Table of Contents

Solution Overview	3
Siebel 8 Application Overview	3
Client Tier	
Application Tier	
Database Tier	
Gateway Name Server	
Radware AppDirector Overview	4
Deployment Notes	5
SIEBEL 8 Load Balancing Application Notes	
Siebel 8 Application Server load balancing rules	
AppDirector and Siebel 8 Architecture	
Diagram 1.0 – Siebel 8 and AppDirector Logical Topology	
Tests Conducted for Solution Validation	
Radware's AppDirector Configuration for Siebel 8 Diagram 2.0 – Siebel 8 and AppDirector Physical Topology	14
Primary AppDirector Configuration	15
IP Configuration	
Farm Configuration	
Create Layer / Policy	
Create Cache Policy	
Create Compression Policy	
Create Layer 4 Policy	
Extended Forme	
Adding Somers to the Form	
Health Monitoring	
General Redundant Configuration Notes	
Primary AppDilector VKKr Configuration	
Primary Virtual Routers	
Philliary Associated IF Addresses	
Backup AppDirector VRRP Configuration	
Backup virtual Koulers	
Appendix 1 – Primary AppDirector Configuration File	
Appendix 2 – Backup AppDirector Configuration File	
Appendix 3 – Insert Cookie - Auto Generated Configuration	

Solution Overview

The Radware and Siebel's joint solution ensures Siebel Business Applications version 8.0 customers solution resilience, efficiency and scale. Radware's AppDirector guarantees Siebel applications maximum availability, scalability, performance and security, managing traffic for both the web server content and application business logic level. AppDirector works in conjunction with Siebel Business applications to offload resource intensive processing, provide advanced health monitoring avoiding system down time and advanced Layer 7 traffic management to deliver a best of breed subsystem. With a pay as you grow platform licensing model, AppDirector ensures long term investment protection facilitating incremental growth demanded by today's Business. Diagram 1.0 is a logical depiction of the intended deployment model.

Siebel 8 Application Overview

Oracle Siebel 8.0 uses a multi-tiered application framework. The Siebel environment consists of client, application, and database tiers. The client tier comprises devices that access the application via the Web. The application tier can be broken down to two different functions, services that terminate client connections and application object managers (AOM) that perform business logic. Multiple application components can reside in the application tier providing different business functions.

Client Tier

There are multiple client types available on the Siebel platform. The major client types are Web client, mobile client, and dedicated Web client. Wireless and handheld clients are used in specialized applications such as retail and manufacturing.

•Siebel Web client—Siebel Web client uses a Web browser on the local PC. It connects to the Siebel Web server via http (port 80) or https (port 443). No additional software is required. The Web client is easy to maintain since it does not require any software upgrades. Since no Siebel software resides on the local PC, it is not affected by software upgrades and updates on the server.

•Siebel mobile client and dedicated client—The mobile client and dedicated client require additional software installed on the PC. The additional software provides faster throughput with less data transfers for a given transaction by sending only changed data between the client and the server. For remote users, the dedicated client allows disconnected mode and synchronizes with the database when network connectivity is restored.

•Siebel wireless client/Siebel handheld client—These two clients are specialized clients for vertical applications. The wireless client has a translator for Hypertext Transfer Protocol (HTTP) to Wireless Application Protocol (WAP), which is suitable for mobile phones. The handheld client can accommodate information on smaller screens.

Application Tier

The application tier contains two functional areas, services that terminate client connections and business logic.

The former component is called the Siebel Web Server Extension (SWSE). It is an add-on to Microsoft Internet Information Server (IIS). SWSE is responsible for handling Web requests from users. It forwards user requests to the Application Object Managers (AOM) via Siebel Internet Session API (SISNAPI) protocol. Siebel provides native server load balancing for highly-available Web servers. Third party load balancers are supported as well.

There are numerous Siebel application servers that provide different business applications. Each Siebel application component can be run on a single or multiple physical servers. Application components can be load balanced at the component level across different physical server pools. Load balancing can be configured with native Siebel load balancer or a third-party load balancer.

Database Tier

The database tier provides a repository to Siebel application data. It consists of a RDBMS and separate file system store.

•File system — The Siebel File System (SFS) is a server with a shared directory that provides CIFS access to other Siebel servers. The SFS is a shared storage area for images, reports, documents, and other data. A pointer in the database record locates the file in the SFS.

•Database Server — The database server is the main data store for the Siebel application. The Siebel application servers connect directly the database server. Oracle 10g is the database used in this deployment.

Gateway Name Server

Gateway name server is a repository for configuration information for each Siebel server. It has configuration information about the Siebel Enterprise.

Radware AppDirector Overview

Radware's AppDirector is an intelligent application delivery controller (ADC) that provides scalability and application-level security for service infrastructure optimization, fault tolerance and redundancy. Radware combined its next-generation, OnDemand Switch multi-gigabit hardware platform with the powerful capabilities of the company's APSolute[™] operating system "classifier" and "flow management" engine. The result – AppDirector – enables accelerated application performance; local and global server availability; and application security and infrastructure scalability for fast, reliable and secure delivery of applications over IP networks.

AppDirector is powered by the innovative OnDemand Switch platform. OnDemand Switch, which has established a new price/performance standard in the industry, delivers breakthrough performance and superior scalability to meet evolving network and business requirements. Based on its on demand, "pay-as-you-grow" approach, no forklift upgrade is required even when new business requirements arise. This helps companies guarantee short-term and long-term savings on CAPEX and OPEX for full investment protection. Radware's OnDemand Switch enables customers to pay for the exact capacity currently required, while allowing them to scale their ADC throughput capacity and add advanced application-aware services or application acceleration services on demand to meet new or changing application and infrastructure needs. And it does it without compromising on performance.

AppDirector lets you get the most out of your service investments by maximizing the utilization of service infrastructure resources and enabling seamless consolidation and high scalability. AppDirector's throughput licensing options allows pay as you grow investment protection. Make your network adaptive and more responsive to your dynamic services and business needs with AppDirector's fully integrated traffic classification and flow management, health monitoring and failure bypassing, traffic redirection, bandwidth management, intrusion prevention and DoS protection.

For more information, please visit: http://www.radware.com/

Deployment Notes

SIEBEL 8 Load Balancing Application Notes

With Siebel 8.0, you can choose between 2 deployment options for load balancing with AppDirector:

Option 1

• AppDirector receives requests from client browsers and load balances them across Siebel Web servers. Load balancing Siebel web servers does not require any specific configuration changes on the web server. The AppDirector appliance can be placed in front of the Web servers and can load balance requests.

• Siebel Load balancing for Application servers; In this case, each Web server is directly tied to an application server.

Note: Siebel Server Load Balancing for Application servers is typically done after the Siebel Servers and Database Server have been installed, but can be done before the Web servers are installed. The Siebel Load Balancing instance resides in the Siebel Web Server Extension (SWSE) on the Web Servers. It allows each instance of SWSE to distribute connection requests to multiple application servers in a round-robin fashion. Typically, the Siebel administrator will generate the load balancing configuration file by logging into the Server Manager and type "generate lbconfig". This generates a load balancing configuration file in the SIEBEL_INSTALLATION_ROOT/Admin directory.



Option 2 – Chosen for Radware Validation Testing

• AppDirector receives requests from client browsers and load balances across Siebel Web servers.

• AppDirector receives application server requests from all Siebel Web servers and load balances to multiple Siebel Application servers.

Note: To implement a hardware based load balancer for Siebel Application servers, a couple of configuration changes on the Siebel Web servers are required.

1. First, update the eapps.cfg file to disable Siebel Load Balancing by changing the setting below as follows:

EnableVirtualHosts = False

2. Next, modify the Object Manager connect string so it points to the Virtual IP and Port. For the load balanced Object Manager, the connect string must have the format:

ConnectString = siebel.TCPIP.None.None://<VirtualIP>:<VirtualPort>/<Siebel Enterprise Name>/<Alias of the Object Manager>

Where:

<VirtualIP>

is the IP address of the Virtual IP (VIP) specified in AppDirector.

This VIP will be assigned to the Application Server Farm.

<VirtualPort>

is the Port Number, or Service defined in the Layer 4 policy VIP definition.

The default port is 2321.

<Siebel Enterprise Name>

is the name of the Siebel Enterprise in which the load balanced Siebel Servers reside.

<Alias of the Object Manager>

is the alias of the Load Balanced Object Manager.

Example eapps.cfg:

Before required changes

EnableVirtualHosts = true

[/callcenter_enu]

ConnectString = siebel.TCPIP.None.None://VirtualServer/SBA_80/SCCObjMgr_enu

After required changes

EnableVirtualHosts = false

[/callcenter_enu]

ConnectString = siebel.TCPIP.None.None://10.10.10.55:2321/SBA_80/SCCObjMgr_enu



Logical Architecture for Option 2

Note: Each URL and OM connect string typically corresponds to one Siebel Application. It will not work to have the same application referencing multiple VIPs in the AppDirector. VIPs can be shared between applications but any one application should only reference one VIP.

Siebel 8 Application Server load balancing rules

Developing the load balancing rules for AppDirector to direct traffic to the Siebel Application Tier requires an understanding of the "lbconfig" file generated for Siebel local load balancing by the SWSE.

There are three rules that need to be defined:

- 1. The first time a request is established for a new connection.
- 2. When the server needs to reconnect back to the same server after a disconnect occurs
- 3. When the Siebel Broker detects that no AOM is available that the request should be Round Robin load balanced to the next broker to handle the request.

Here is a sample section of the "lbconfig" file

This is the load balance configuration file generated by the Siebel srvrmgr "generate lbconfig" command.

It contains two sections. Section one contains load balancing rules to be used by Siebel session manager.

Section two is intended for 3rd party load balancers. Before modifying the content of this file please

read the chapter on SWSE configuration in the Siebel Bookshelf.

#Section one -- Session Manager Rules:

VirtualServer=1:siebelrw:2321;5:siebelrw1:2321;

#Section two -- 3rd Party Load Balancer Rules

/SBA_80/SCCObjMgr_enu=siebelrw1:2321;siebelrw:2321;

#Server Rules:

/!1.=siebelrw:2321;

/!5.=siebelrw1:2321;

#Round Robin Rules:

/SBA_80/SCCObjMgr_enu/RR=siebelrw1:2321;siebelrw:2321;

Explanation of the "lbconfig" file

The first section identifies the Siebel application servers and the port the broker is listening on.

VirtualServer=1:siebelrw:2321;5:siebelrw1:2321;

The string "1:siebelrw:2321;5:siebelrw1:2321" has the following meaning:

- 1 is assigning to the server siebelrw and 5 is assigning to the server siebelrw1
- siebelrw is the host name and translates to IP 10.10.10.53 and siebelrw1 to IP 10.10.10.50
- 2321 is the port that the Broker is listening on.

When the AppDirector reads the URL sent from the SWSE to determine what action to take when directing traffic to the Siebel Server requires the setup of three server farms:

• One containing siebelrw:2321;siebelrw1:2321, this will be used to load balance The first time a request is established for a new connection and when a connecting is rejected by a Broker and the SWSE sends a request to the AppDirector to round robin the request to a new broker.

The next two farms are used when the server needs to reconnect back to the same server after a disconnection occurs, L7 URI persistence. This is a one to one mapping of the URI to a Farm containing a single server.

- one containing siebelrw:2321
- one containing siebelrw1:2321

The SWSE injects into the URI a "!1" or "!5" to identify the server that the request should be sent to.

/<mark>!1</mark>.=siebelrw:2321; IP 10.10.10.53 */<mark>!5</mark>.*=siebelrw1:2321 IP 10.10.10.50

The SWSE injects into the URI a "RR" to identify that the request should be re-load balanced round robin to the next available broker.

/SBA_80/SCCObjMgr_enu/RR=siebelrw1:2321;siebelrw:2321

AppDirector and Siebel 8 Architecture

Key features implemented on the AppDirector to support this solution:

- Service health monitoring
- Layer 4 load balancing
- Layer 7 load balancing
- Cookie based Persistence
- Caching
- Compression
- Client NAT
- Server NAT
- VRRP



Diagram 1.0 – Siebel 8 and AppDirector Logical Topology

Tests Conducted for Solution Validation

The following tests were conducted to ensure the most appropriate solution was defined and validated. All tests were successfully completed using the AppDirector and Oracle Siebel 8 configurations following Table 1.0.

Test Case	Action	Expected Result	Actual Result	Status
Siebel Web Client Login Page	 Open Browser Window Paste the following web URL "HTTP:// 76.197.19.55 /callcenter_enu 	Siebel Login Page should Display	Siebel Login Page is displayed	Pass
Siebel Web Client Home Page	 Provide Login name as SADMIN, Password : SADMIN 	Siebel Home Page should Display after successful Login	Siebel Home Page is displayed	Pass
Siebel Server Administrati on Screen	 Click on Site Map Check for the Siebel server Check for the running instances of all the Siebel components like Request Broker, Request Processor, Transaction Manager etc., 	 Click on Site Map Check for the Siebel server Check for the running instances of all the Siebel components like Request Broker, Request Processor, Transaction Manager Click on Site Map Siebel should show the Running instance of Servers and Components Siebel should show the Running instance of Servers and Components 		Pass
Create an opportunity record	 Click on Site Map Click on Opportunity Select Opportunity List Click on New Button (or use Applet Menu or Ctrl + N to create a new Record) Provide Opportunity Name, Sales Stage (Write whatever the required fields are in Opportunity) Open Applet Menu and Click on "Save Record" Or Press ^S 	The Opportunity should be saved. And displayed in the UI	The Opportunity is created and saved. It is also displayed in the UI	Pass
Query an opportunity record	 Click on Site Map Click on Opportunity Select Opportunity List Click on Query Button Provide Opportunity Name and click Go button 	The Opportunity should be displayed in the UI	The Opportunity is displayed in the UI	Pass
Delete an opportunity record	 Click on Site Map Click on Opportunity Select Opportunity List Click on Query Button Provide Opportunity Name and click Go button Highlight the Opportunity record and click Delete button. 	The Opportunity should be deleted.	The Opportunity is deleted and not displayed in the UI	Pass
Siebel Dedicated	 Open Siebel Application using the Siebel client shortcut key on the 	Siebel Login Page should Display	Siebel Login Page is displayed	Pass

Client	programs list	properly		
Siebel Web Server Load Balance	 Open Browser Window At least 6 users should log in to the Siebel web client Provide Login name and password for the 6 different instances 	Siebel Login Page should Display Siebel Home Page should Display after successful Login for all the six users	Siebel Home Pages are displayed after successful Login for all the six users Web Server 1 has 3 users connected and Web Server 2 has 3 users connected	Pass
Siebel App Server Load Balance	 Open Browser Window At least 6 users should log in to the Siebel web client Provide Login name and password for the 6 different instances 	Siebel Login Page should Display Siebel Home Page should Display after successful Login for all the six users	Siebel Home Pages are displayed after successful Login for all the six users Siebel Server Manager shows Siebel App Server 1 has 3 user sessions and Siebel App Server 2 has 3 user sessions	Pass
Siebel Web Server Session Persistence	 Open Browser Window At least 6 users should log in to the Siebel web client Provide Login name and password for the 6 different instances 	Siebel Login Page should Display Siebel Home Page should Display after successful Login for all the six users Siebel Web Server Sessions should be persistent	Siebel Web Server Sessions are persistent based on Radware Inserted HTTP session cookies Radware AD shows all requests within same session are routed to same Web Server.	Pass
Siebel App Server Retry	 Siebel App Server 1 has MaxTasks=3 Siebel App Server 2 has MaxTasks=20 Open Browser Window At least 10 users should log in to the Siebel web client Provide Login name and password for the 10 different instances 	Siebel Login Page should Display Siebel Home Page should Display after successful Login for all the 10 users	Siebel Home Pages are displayed after successful Login for all the 10 users Siebel Server Manager shows Siebel App Server 1 has 3 user sessions and Siebel App Server 2 has 7 user sessions Web Server 1 has 5 users connected and Web Server 2 has 5 users connected Radware AD shows 2 matches of retry policy rule for App Server 1	Pass
Siebel App Server	Open Browser WindowProvide Login name as	Siebel Login Page	Siebel Home Page	Pass

Reconnect	SADMIN, Password: SADMIN	should Display Siebel Home Page should Display after successful Login	successful Login Radware AD shows 1 match of reconnect policy rule for App Server 1 (when switch from anonymous user session to actual user session)	
Health Check: Web Server Failure	 Shutdown IIS service on Web Server 1 Open Browser Window Provide Login name as SADMIN, Password: SADMIN 	Siebel Web Server 1 should be taken out from Radware Web Server Farm Siebel Login Page should Display Siebel Home Page should Display after successful Login	Radware AD shows "Not in Service" for Web Server 1 Siebel Home Page is displayed after successful Login	Pass
Health Check: Siebel App Server Failure	 Stop Siebel App Server 1 Open Browser Window Provide Login name as SADMIN, Password: SADMIN 	Siebel App Server 1 should be taken out from radware App Server Farm Siebel Login Page should Display Siebel Home Page should Display after successful Login	Radware AD shows "Not in Service" for App Server 1 Siebel Home Page is displayed after successful Login	Pass
Siebel Web Client Session Timeout	 Login to the web client with the appropriate user name and password Leave the session open for 60 min 	Siebel Home Page should Display after successful Login and should be open for the entire session 60 min	Siebel Home Page is displayed after successful Login The Siebel session is opened for 60 minutes and then timeout closed.	Pass

Table 1.0 - Test Conducted for Solution Validation

Radware's AppDirector Configuration for Siebel 8

Siebel Server Name	Service	Port	Network IP Address
siebelrw1	web	80	10.10.10.50
siebelrw1	web	80	10.10.10.53
siebelrw1	application broker/AOM	2321	10.10.10.50
siebelrw1	application broker/AOM	2321	10.10.10.53
VIP			
web virtual IP	web	80	76.197.19.55
Application Broker/AOM virtual IP	application broker/AOM	2321	10.10.10.55
one to one virtual IP -10.10.10.50			76.197.19.50
one to one virtual IP - 10.10.10.53			76.197.19.53
Primary AppDirector Routing table and interface IP's	interface	subnet	Network IP Address
Gateway	G-1	255.255.255.0	76.197.19.62
Subnet	G-11	255.255.255.0	10.10.10.0
Subnet	G-1	255.255.255.240	76.197.19.48
Management Interface	MNG-1	255.255.255.0	192.168.1.50
G-11 Interface	G-11	255.255.255.0	10.10.10.1
G-1 Interface	G-1	255.255.255.240	76.197.19.61

Backup AppDirector Routing table and interface IP's	interface	subnet	Network IP Address
Gateway	G-1	255.255.255.0	76.197.19.62
Subnet	G-11	255.255.255.0	10.10.10.0
Subnet	G-1	255.255.255.240	76.197.19.48
Management Interface	MNG-1	255.255.255.0	192.168.1.53
G-11 Interface	G-11	255.255.255.0	10.10.10.3
G-1 Interface	G-1	255.255.255.240	76.197.19.60



Diagram 2.0 – Siebel 8 and AppDirector Physical Topology

Primary 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

 Using the following Command line, assign management IP address 192.168.1.50 / 24 to interface 17 (Dedicated Management Interface) of the AppDirector:

net ip-interface create 192.168.1.50 255.255.255.0 MNG-1

2. Using a browser, connect to the management IP Address of the AppDirector (192.168.1.50) via HTTP or HTTPS. The default username and password are "radware" and "radware".

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

🐮 radware	AppDirector with Cookie Persistency	000
Status:		
File Device		
Bridge Router	AppDirector XA, egg 41 - 22 - 52 - 61 - 63 - 61 - 94 - 15 - 940 - 47 - 47 - 47 - 47 - 47 - 47 - 47 -	
AppDirector Health Monitoring		
Security Classes		
Performance Services		
Help		

IP Configuration

1. From the menu, select **Router** ⇒ **IP Router** ⇒ **Interface Parameters** to display the **IP Interface Parameters** page similar to the one shown below:

IP Interface Parameters

Routing Tab	le	ARP Table						
			IP Interface F	arame	ters			
		IP Address	Network Mask	If Nu	mber	VlanTag	×	
		<u>192.168.1.50</u>	255.255.255.0	MNG	-1	0		
				D	elete	Crea	ate	
			ICMP Interface	Param	neters			
IP Address	Adv	vert. Address	Max Advert. Int	erval	Min /	Advert. Inte	erval	Advert. Lifetime
<u>192.168.1.50</u>	224	.0.0.1	600		450			1800

- 2. Click the **Create** button.
- 3. On the **IP Interface Parameters Create** page, enter the necessary parameters as shown below:¹

IP Interface Parameters Create

Routing Table	ARP Table		
IP Address:	(76.197.19.61)	Network Mask:	255.255.255.240)
If Number:	G-1 💌	Fwd Broadcast:	enable 💌
Broadcast Addr:	ONE FILL	VlanTag:	0
	Set	Cancel	

- 4. Click the Set button to save parameters.
- 5. On the **IP Interface Parameters** page, click the **Create** button to configure another interface. enter the necessary parameters as shown below:

¹ Items circled in red indicate settings that need to be entered or changed. Items not circled should be left to default settings.

IP Interface Parameters Create

Routing Table	ARP Table		
IP Address:	(10.10.10.1	Network Mask:	255.255.255.0)
If Number:	G-11) 🗸	Fwd Broadcast:	enable 💌
Broadcast Addr:	ONE FILL	VlanTag:	0
	Set	Cancel	

- 6. Click the **Set** button to save parameters.
- 7. Verify that the new entries were created on the IP Interface Parameters page:

IP Interface Parameters

Routing Table ARP Table

IP Interface Parameters						
IP Address	Network Mask	If Number	VlanTag	×		
<u>10.10.10.1</u>	255.255.255.0	G-11	0			
<u>76.197.19.61</u>	255.255.255.240	G-1	0			
<u>192.168.1.50</u>	255.255.255.0	MNG-1	0			
		Delete	Crea	ate		

ICMP Interface Parameters

IP Address	Advert. Address	Max Advert. Interval	Min Advert. Interval	Advert. Lifetime
<u>10.10.10.1</u>	224.0.0.1	600	450	1800
76.197.19.61	224.0.0.1	600	450	1800
<u>192.168.1.50</u>	224.0.0.1	600	450	1800

Farm Configuration

1. From the menu, select **AppDirector** ⇒ **Farms** ⇒ **Farm Table** to display the **Farm Table** page similar to the one shown below:

Farm Table							
Extended Farm Pa	arameters	Layer 4 Policy Tal	ble Server Tabl	le DNS Persistency Param	eters Table	Redirection Table	Windows NT Parameters
Private Paramete	rs						
Earner Marra	A daylar Cont			Commentation Character Marthand	C 14		
Farm Name		tus Aging Time	Dispatch Method	Соппесалану спеск метноа	Sessions M	ode Oper	ational status 🔺
						De	elete Create

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

Farm Table Create						
Extended Farm Paramete	rs Layer 4 Policy Table	Server Table	DNS Persister	cy Parameters Table	Redirection Table	Windows NT Parameters
Private Parameters						
Farm Name:	web server farm)	Admin Stat	us:	Enabled 💌		
Aging Time:	7300	Dispatch M	ethod:	Cyclic	*	
Connectivity Check Method:	No Checks 🎽	Sessions N	lode:	RemoveOnSessionEnd	SPS) V	
Bandwidth Limit:	No Limit	Connectivity	/ Check Port:	HTTP	~	
Connectivity Check Interval:	10	Connectivity	Check Retries:	5		
Extended Check Frequency:	10	Home Page	e.			
Authorized Username:		Authorized	Password:			
	Se	tCancel				

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

Farm Table Create

5. On **Farm Table** page Click the **Create** button to configure another interface. enter the necessary parameters as shown below:

Extended Farm Paramete	rs Layer 4 Policy Table	Sei	rver Table	DNS Persister	cy Parameters Table	Redire	ction Table	Windows NT Parameters
Private Parameters								
Farm Name:	App_Server_Farm)		Admin Stati	us:	Enabled 💌			
Aging Time:	7300		Dispatch M	ethod:	Cyclic		~	
Connectivity Check Method:	No Checks 😽		Sessions M	lode:	(ServerPerSession)	*		
Bandwidth Limit:	No Limit	*	Connectivity	/ Check Port:	HTTP	~		
Connectivity Check Interval:	10		Connectivity	/ Check Retries:	5			
Extended Check Frequency:	10		Home Page					
Authorized Username:			Authorized	Password:				
	Set		Cancel					

- 6. Click the Set button to save parameters.
- 7. On **Farm Table** page Click the **Create** button to configure another interface. enter the necessary parameters as shown below:

Farm Table Create							
Extended Farm Paramete	rs Layer 4 Policy Table	Server	Table DNS I	Persistency Pa	arameters Table	Redirection Table	Windows NT Parameters
Private Parameters							
Farm Name:	Server_50_Farm	Adn	min Status:	Ena	bled 🎽		
Aging Time:	7300	Disp	patch Method:	Cyc	lic	*	
Connectivity Check Method:	Ping 🎽	Ses	ssions Mode:	Sen	verPerSession	*	
Bandwidth Limit:	No Limit	🖌 Con	nnectivity Check	Port: HTTP	P	~	
Connectivity Check Interval:	10	Con	nnectivity Check	Retries: 5			
Extended Check Frequency:	10	Hon	me Page:				
Authorized Username:		Aut	thorized Passwo	ord:			
	Set	t Ca	ancel				

- 8. Click the **Set** button to save parameters.
- 9. On **Farm Table** page Click the **Create** button to configure another interface. enter the necessary parameters as shown below:

Extended Farm Parameter	rs Layer 4 Policy Table	Server Table	DNS Persiste	ncy Parameters Table	Redirection Table	Windows NT Parameters
Private Parameters						
Farm Name:	Server_53_Farm	Admin S	tatus:	Enabled 😽		
Aging Time:	7300	Dispatch	Method:	Cyclic	*	
Connectivity Check Method:	Ping 💙	Session	Mode:	ServerPerSession	*	
Bandwidth Limit:	No Limit	V Connect	vity Check Port:	HTTP	~	
Connectivity Check Interval:	10	Connect	vity Check Retries:	5		
Extended Check Frequency:	10	Home Pa	age:			
Authorized Username:		Authoriz	ed Password:			

10. Verify that the new entries are created on the Farm Table page:

Farm Table									
Extended Farm Pa	rameters l	Layer 4 Policy Ta	able Server Tab	le DNS Persistency Param	eters Table	Redirection T	able Windows N	T Parameters	Private Parame
Farm Name	Admin Statu	us Aging Time	Dispatch Method	Connectivity Check Method	Sessions Mo	ode	Operational Statu	5 🗙	
<u>web server farm</u>	Enabled	7300	Cyclic	No Checks	RemoveOnS	essionEnd-SPS	Active		
App_Server_Farm	Enabled	7300	Cyclic	No Checks	ServerPerSe	ssion	Active		
Server_50_Farm	Enabled	7300	Cyclic	Ping	EntryPerSes	sion	Active		
Server_53_Farm	Enabled	7300	Cyclic	Ping	EntryPerSes	sion	Active		
							Delete Cr	eate	

Create Layer 7 Policy

Note: AppDirector needs to be configured with L7 rules in order to load balance Seibel application layer.

There are three rules that need to be defined:

- 1. The first time a request is established for a new connection.
- 2. When the server needs to reconnect back to the same server after a disconnect occurs
- 3. When the Siebel Broker detects that no AOM is available that the request should be Round Robin load balanced to the next broker to handle the request.

Methods Table

The Methods are created to map to the three rules described above.

1. From the menu, select **AppDirector** ⇒ **Layer 7** Farm Selection ⇒ Methods to display the Methods Table page similar to the one shown below:

Method Table				
Layer 7 Policy Table	Layer 7 Policy Sta	tistics	Layer 7 Modification Table	
Method Name	Method Type	Argum	ents	×
			Delete	Create

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

Method Table Create

Layer 7 Policy Table	Layer 7 Policy Statistics	Layer 7 Modification Table
Method Name: RR	Л	/lethod Type: (Regular Expression) 🗸
Arguments: EXP=.*/F	RR*	
	Set Cance	el
4. Select the 🛄 to	enter in the arguments	s below
Arguments for Regular	Expression Method	
Regular Expression: .*/R	R*	
Set	Cancel	

- 5. Click the **Set** button to save the parameters.
- 6. On **Methods Table** page Click the **Create** button to configure another method. Enter the necessary parameters as shown below

Method Table Create

Layer 7 Policy T	able Layer 7 Policy	Statistics	Layer 7 Modification Table
Method Name: A	ppSrv50	Met	thod Type: (Regular Expression) 🗸
Arguments:	XP=.*/!5.*)		
	Set	Cancel	
7. Select the	to enter in the ar	guments	below

Arguments for Reg	ular Expression Method			
Regular Expression:	.*/15.*			
Set	Cancel			

- 8. Click the **Set** button to save the parameters.
- 9. On **Methods Table** page Click the **Create** button to configure another method. Enter the necessary parameters as shown below

Method Table Create

Layer 7 Policy Table	Layer 7 Policy Statistic	s Layer 7	Modification Table
Method Name: AppSrv53	3	Method Type:	(Regular Expression) 🗸
Arguments: EXP=.*/!	1.*		
	Set Can	cel	
10. Select the 🛄 to	enter in the argumen	its below	
Arguments for Regular	Expression Method		
Regular Expression: .*/!1.*	¢		
Set C	Cancel		

- 11. Click the **Set** button to save the parameters.
- 12. On **Methods Table** page Click the **Create** button to configure another method. Enter the necessary parameters as shown below

Method Table Create

Layer 7 Policy Table	Layer 7 Policy Statistic	s Layer 7 Modification Table
Method Name: LBAppSr	v I	Method Type: Regular Expression 👻
Arguments: EXP=.*)	
	Set Canc	el
13. Select the 🛄 to	enter in the argumen	ts below
Arguments for Regular	Expression Method	
Regular Expression: .*		
Set	Cancel	

- 14. Click the **Set** button to save the parameters.
- 15. Verify that the new entries were created on the **Methods Table** page:

Method Table			
Layer 7 Policy Table	Layer 7 Policy Sta	tistics Layer 7 Modification Table	
Method Name	Method Type	Arguments	×
AppSrv50	Regular Expression	EXP=.*/!5.*	
AppSrv53	Regular Expression	EXP=.*/!1.*	
LBAppSrv	Regular Expression	EXP=.*	
RR	Regular Expression	EXP=.*/RR*	
		Delete Cre	ate

Note: The layer 7 policies define the order for which the rules will be evaluated and to what farm the request will be sent when matched.

16. From the menu, select **AppDirector** ⇒ **Layer 7** Farm Selection ⇒ Policies to display the Layer 7 Policies Table page similar to the one shown below:

Layer 7 Policy Table

Layer 4 Polic	y Table Mo	ethod Table	Layer 7 Policy Stat	tistics	
Policy Name	Policy Index	First Method	Second Method	Farm Name	×
				Delete	Create

- 17. Click the **Create** button
- 18. On the **Policy Table Create** page, enter the necessary parameters as shown below

Layer 7 Policy Table	Create		
Layer 4 Policy Table	Method Table	Layer 7 Policy Stat	istics
Policy Name: (App_lb)		Policy Index:	(1)
First Method: (RR)	~	Second Method:	
Arguments: PRSST=Or	n)	Farm Name:	App_Server_Farm
	Set	Cancel	
19. Select the 🛄 to	enter in the arc	guments below	
Argument	ts for Policy		
Retain HTTP Persistency	y: On 🗸		
HTTP Redirect To:			
HTTPS Redirect To:			
SIP Redirect To:			
Ŧ	×		
Set	Cancel		

- 20. Click the **Set** button to save the parameters.
- 21. On Layer 7 Policies Table page Click the Create button to configure another policy. Enter the necessary parameters as shown below.

Layer 7 Policy Tabl	e Create		
Layer 4 Policy Table	Method Table	Layer 7 Policy Stati	stics
Policy Name: App_lb		Policy Index:	6
First Method: AppSrv53	~	Second Method:	~
Arguments: (PRSST=C	Dn	Farm Name:	(Server_53_Farm) 💌
	Set	Cancel	
22. Select the 🛄 t	o enter in the a	rguments below	
Argume	nts for Policy		
Retain HTTP Persisten	ıcy: On 🗸		
HTTP Redirect To:			
HTTPS Redirect To:			
SIP Redirect To:			
Ŧ			
Set	Cancel		

- 23. Click the **Set** button to save the parameters.
- 24. On **Layer 7 Policies Table** page Click the **Create** button to configure another policy. Enter the necessary parameters as shown below.

Layer 7 Policy Table Create

Layer 4 Policy Table	Method Table	Layer 7 Policy Stati	stics
Policy Name: App_lb First Method: AppSrv50)	Policy Index: Second Method:	7 •
Arguments: PRSST=0	n)	Farm Name:	Server_50_Farm
	Set	Cancel	
25. Select the 🛄 to	enter in the ar	guments below	
Argumen	ts for Policy		
Retain HTTP Persistence	y: <mark>On </mark> ♥		
HTTP Redirect To:			
HTTPS Redirect To:			
SIP Redirect To:			
Set	Cancel		

- 26. Click the **Set** button to save the parameters.
- 27. On **Layer 7 Policies Table** page Click the **Create** button to configure another policy. Enter the necessary parameters as shown below.

Layer 7 Policy Table Create

	Layer 4 Policy Table	Method Table	Policy Stati	stics			
	Policy Name: App_lb First Method: LBAppSr Arguments: PRSST=0	v v	Pol See	licy Index: cond Method: m Name:	(10)	_Server_Farm	*
		Set	Cano	cel			
2	28. Select the 🛄 to	o enter in the ar	guments	below			
	Argume	nts for Policy					
	Retain HTTP Persisten	icy: On 🗸					
	HTTP Redirect To:						
	HTTPS Redirect To:						
	SIP Redirect To:						
) 🗶					

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

Cancel

Set

30. Verify that the new entries were created on the Layer 7 Policies Table page:

Layer 7 Policy Table

Layer 4 Polic	y Table Me	thod Table	Layer 7 Policy Sta	tistics	
	D P I I			F 11	N
Policy Name	Policy Index	First Method	Second Method	Farm Name	×.
App_lb	1	RR		App_Server_Farm	
App_lb	5	AppSrv53		Server_53_Farm	
App_lb	7	AppSrv50		Server_50_Farm	
App_lb	10	LBAppSrv		App_Server_Farm	
				Delete Crea	ate

Create Cache Policy

From the menu, select AppDirector
 ⇒ Layer 4 Traffic Redirection
 ⇒
 Caching Policy to display the AppDirector Caching Policy page similar to
 the one shown below:

AppDirector Caching Policy

Layer 4 Policy	y Table	Layer 7 Pol	icy Table	Compression Policy Table
Cach	e purge: a	all	•	
		Set		
A	ppDirecto	r Caching Poli	cy	
Policy Name	Admin S	Status Expira	tion [sec]	×
		Delete	Crea	ite

- 2. Click the **Create** button.
- 3. On the **AppDirector Caching Policy Create** page, enter the necessary parameters as shown below.

AppDirector Caching Policy Create

Layer 4 Policy	Table	Layer 7	Policy T	able	Compre	ession Po	licy Table
Policy Name:	Siebel			Admir	n Status:	Enabled	•
Expiration [sec]:	86400						
	I	Set	Canc	el			

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

Create Compression Policy

From the menu, select AppDirector
 ⇒ Layer 4 Traffic Redirection
 ⇒
 Caching Policy to display the AppDirector Caching Policy page similar to
 the one shown below:

AppDirector Compression Policy

Layer 4 Polic	y Table	Layer 7 Policy Table	Caching P	olicy Ta	able	
Policy Name	Algorithm	n Compression Level	Min Size (B	ytes)	Engine	×
			D	elete	Crea	ate

- 2. Click the **Create** button.
- 3. On the **AppDirector Caching Policy Create** page, enter the necessary parameters as shown below.

AppDirector Compression Policy Create

Layer 4 Policy Table	e Layer 7 Policy Tab	le Caching Poli	cy Table
Policy Name:	Siebel)	Algorithm:	GZIP 💌
Compression Level:		Min Size (Bytes):	1024
Engine:	Hardware		
	Set	Cancel	

Note: this version of hardware support hardware compression.

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

Create Layer 4 Policy

 From the menu, select AppDirector
 ⇒ Layer 4 Traffic Redirection
 ⇒ Layer 4
 Policy Table to display the Layer 4 Policy Table page similar to the one
 shown below:

Layer 4 Poli	cy Table															?
Farm Table	Layer 7 Policy	Table S	SSL Policy	Table	Cachi	ng Policy Tał	ble	Compre	ssion Policy 1	Table	Clie	ent Authentication F	Policy Table	Layer 4 Policy Sta	atistics	1
Virtual IP	L4 Policy Name	L4 Protocol	L4 I Port	Source From	e IP	Source IP To	L7 P Nam	olicy Ie	Farm Name	SSL Policy	y	Compression Policy	Caching Policy	Client Authentica Policy	ition	×
														Delete	Crea	ate

2. Click the **Create** button.

3. On the Layer 4 Policy Table Create page, enter the necessary parameters as shown below.

Farm Table Layer 7 Policy Table S	SL Policy Table	Caching Policy Table	Compression Policy Table	Client Authentication Policy Table	Layer 4 Policy Statistics
L4 Policy Name: (WebServiceHTTP)					
Virtual IP: (76.197.19.55)		L4 Protocol:	TCP -		
L4 Port: 80	•	Source IP From:	0.0.0.0		
Application: (HTTP) -		Source IP To:	0.0.0.0		
				7	
Farm Name: (web server farm) 🔻		L7 Policy Name:	None -		
SSL Policy: None -		Client Authenticat	ion Policy: None -		
Caching Policy: Siebel) -		Compression Poli	cy: Siebel -		
Redundancy Status: Primary 🔻		POOT OL	and the state	-	
Bytes of Request to Read: 3584		POST Classificati	on input: Header		
L7 Persistent Switching Mode: (Maintain)	-	HTTP Normalizatio	on: Disabled 🔻		
		Set Cancel			

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

Laver 4 Policy Table Create

5. On **Layer 4 Policy Table** page Click the **Create** button to configure another L4 Policy. Enter the necessary parameters as shown below:

Farm Table Layer 7 Policy Table SSL Policy Table Caching Po	licy Table Compression Policy Table Client Authentication Policy Table Layer 4 Policy Statist
.4 Policy Name: (Siebel_Server_50)	
Virtual IP: (76. 197. 19.50) .4 Port: Any Application: Any	L4 Protocol: Any Source IP From: 0.0.0.0 Source IP To: 0.0.0.0
Farm Name: (Server_50_Farm) v SSL Policy: None v Caching Policy: None v	L7 Policy Name: None Client Authentication Policy: None Compression Policy: None
Primary Bytes of Request to Read 3584 .7 Persistent Switching Mode: First	POST Classification Input: Header

- 6. Click the **Set** button to save the parameters.
- 7. On **Layer 4 Policy Table** page Click the **Create** button to configure another L4 Policy. Enter the necessary parameters as shown below:

Layer 4 Policy Table Create

4 Policy Name: (Siebel_Serve	er_53)			
Virtual IP: (76.197.19.53)		L4 Protocol: (Any) -		
L4 Port: Any	•	Source IP From: 0.0.0.0		
Application: Any		Source IP To: 0.0.0.0		
Farm Name: Server_53_F SSL Policy: None Caching Policy: None	arm) 🔹	L7 Policy Name: Client Authentication Policy: Compression Policy:	None Vone Vone	
Redundancy Status: Bytes of Request to Read:	Primary • 3584	POST Classification Input:	Header •	
L7 Persistent Switching Mode:	First 👻	Hit Hornaizaton.		
8		Set Cancel		

 Farm Table
 Layer 7 Policy Table
 SSL Policy Table
 Caching Policy Table
 Compression Policy Table
 Client Authentication Policy Table
 Layer 4 Policy Statistics

- 8. Click the **Set** button to save the parameters.
- 9. On **Layer 4 Policy Table** page Click the **Create** button to configure another L4 Policy. Enter the necessary parameters as shown below:

arm Table Layer 7 Pol	icy Table	SSL Policy Table	Caching Policy Table	Compression	Policy Table	Client Authe	ntication Policy Table	Layer 4 Policy Stati
Policy Name: App_svr_17)							
rtual IP: (10.10.10.55)			L	4 Protocol:	TCP 💌			
4 Port: Any pplication: Any	~	v	5	Source IP From:	0.0.0.0			
arm Name: (None)	*		t	.7 Policy Name:	Œ	.pp_lb)		
SL Policy: None 💌			(Client Authenticat	ion Policy: N	ione 💙		
dundancy Status:	Primary	2					1	
ytes of Request to Read: 7 Persistent Switching Mod	3584		ŀ	HTTP Normalizatio	on input: Her	ader 👻	1	

Note: The Layer 7 policy "App_lb" needs to be created first in order to select it in the Layer 4 Policy Table.

10. Verify that the new entries were created on the Layer 4 Policy Table page:

Layer 4 Policy Table

Tann Table	Luyer r oncy ro	1016 00L1	oncy rubi	e caching i or	icy rubic co	inpression roncy	Tuble Chefit A	unionacation	Toncy Table Layer	41 oney statistic	<u> </u>	
Virtual IP	L4 Policy Name	L4 Protocol	L4 Port	Source IP From	Source IP To	L7 Policy Name	Farm Name	SSL Policy	Compression Policy	Caching Policy	Client Authentication Policy	×
10.10.10.55	App_svr_17	TCP	2321	0.0.0.0	0.0.0.0	App_lb	None	None	None	None	None	
76.197.19.50	Siebel_Server_50	Any	Any	0.0.0.0	0.0.0.0	None	Server_50_Farm	None	None	None	None	
76.197.19.53	Siebel_Server_53	Any	Any	0.0.0.0	0.0.0.0	None	Server_53_Farm	None	None	None	None	
76.197.19.55	WebServiceHTTP	TCP	80	0.0.0.0	0.0.0.0	None	web server farm	None	Siebel	Siebel	None	
											Delete Cre	ate

Configure NAT

Server NAT

- From the menu, select AppDirector ⇒ NAT ⇒ Server NAT ⇒ Global Parameters to display the Server NAT - Global Parameters page similar to the one shown.
- 2. Enable Server NAT and click the Set button to save parameters.

Server NAT - Global Parameters

Device Tuning	
Server NAT:	enable -
Use Specific NAT Address:	• 0.0.0.0
Set	

Client NAT

In addition to the configurations below, you must enable Client NAT in the **Extended Farms Table** and in the **Server Table** Configuration.

- 1. From the menu, select **Services** ⇒ **Tuning** ⇒ **Device** to display the **Device Tuning** page similar to the one shown.
- 2. Adjust the number of allowable Client NAT address to the desired amount, at least one and click the **Set** button to save parameters.

Device Tuning

Memory Check Tunable Tables Usage Statistics

Bridge Forwarding Table:	1024	Bridge Forwarding Table After Reset:	1024
IP Forwarding Table:	240000	IP Forwarding Table After Reset:	240000
Arp Forwarding Table:	1024	Arp Forwarding Table After Reset:	1024
Client Table:	120000	0Client Table After Reset:	1200000
Routing Table:	512	Routing Table After Reset:	512
Hosts Table:	256	Hosts Table After Reset:	256
Request Table:	5000	Request Table After Reset:	5000
Client NAT Addresses:	4	Client NAT Addresses After Reset:	4
Client NAT Ports Per Address:	64511	Client NAT Ports Per Address After Reset:	64511
Outbound NAT Addresses:	1	Outbound NAT Addresses After Reset:	1
Outbound NAT Ports Per Address:	64511	Outbound NAT Ports Per Address After Reset:	64511
Outbound NAT Intercept Ranges:	4	Outbound NAT Intercept Ranges After Reset:	4
Session IDs:	32000	Session IDs After Reset:	32000
Layer3 Client Table [% of the client table]:	20	Layer3 Client Table After Reset [% of the client table]:	20
RADIUS Attribute Table:	1	RADIUS Attribute Table After Reset:	1
Network Segments:	15	Network Segments After Reset:	15

Set

The AppDirector must be reset in order for the settings to take effect.

3. To reset the device, From the menu, select **Device** \Rightarrow **Reset Device**

Reset the Device





4. From the menu, select **AppDirector** ⇒ **NAT** ⇒ **Client NAT** ⇒ **Intercept Address** to display the **Client NAT Intercept Table** page similar to the one shown.

Client NAT Intercept Table

Client NAT Global Parameters	Device Tuning	Client NAT Address Table					
From Client IP To Client IP 🔀							

- 5. Click the **Create** button.
- 6. Create the intercept range. On the **Client NAT Intercept Table Create** page, enter the necessary parameters as shown below:

Client NAT Intercept Table Create

Client NAT Global Parameters	Device Tuning	Client NAT Address Table
From Client IP: (10.10.10.50)	To Client IF	P: (10.10.10.53)
Se	tCancel	

- 7. Click the Set button to save parameters.
- 8. From the menu, select **AppDirector** ⇒ **NAT** ⇒ **Client NAT** ⇒ **Intercept Address** to display the **Client NAT Address Table page** similar to the one shown.

Client NAT Address Table

Client NAT Global Parameters	Client NAT Intercept Table	Device Tuning
From IP Address To IP Address	×	
Delete Cre	eate	

- 9. Click the **Create** button.
- 10. Create the NAT Address range. On the **Client NAT Address Table Create** page, enter the necessary parameters as shown below:

Client NAT Address Table Create

Client NAT Global Parameters	Client NAT Intercept Table	Device Tuning
From IP Address: (10.10.10.100)	To IP Address: 10.1	0.10.100)
	Set Cancel	

- 11. Click the **Set** button to save parameters.
- 12. From the menu, select **AppDirector** ⇒ **NAT** ⇒ **Client NAT** ⇒ **Global Parameters** to display the **Client NAT Global Parameters** page similar to the one shown.
- 13. Enable Client NAT and click the **Set** button to save parameters.

Client NAT Global Parameters

Device Tuning	Client NAT Intercept Table	Client NAT Address Table
Client NAT: Enabled	d) -	
Set		

Extended Farms

Configure Client NAT at the farm level

- 1. Click the Extended Farm Parameters URI at the top of the Farm Table page.
- 2. On the **Extended Farm Parameters Table** page, click on the Farm Name Server_50_Farm.
- 3. On the **Extended Farm Parameters Update** page, enter the necessary parameters as shown below:
| Extended Farm Parameters Update | | | | | | | |
|-------------------------------------|----------------|---------------------------------------|------------------|--|--|--|--|
| Farm Table | | | | | | | |
| | | | | | | | |
| Farm Name: | Server_50_Farm | Radius Secret: | | | | | |
| Connection Limit Exception: | Disabled 💌 | Client NAT Address Range: | (10.10.10.100) 🗸 | | | | |
| SSL ID Tracking: | Disabled 💌 | Close Session At Aging: | Disabled 🛩 | | | | |
| RADIUS Attribute: | 0 | Reset Client on Server Failure: | Disabled 🛩 | | | | |
| RADIUS Proxy Attribute: | 0 | Add X-Forwarded-For to HTTP requests: | Disabled 💙 | | | | |
| Insert Cookie for HTTP Persistency: | Disabled | Hash Parameter For SIP: | Call-ID | | | | |
| SSL ID Aging: | 120 | Select Server Per Transaction: | Disabled 🛩 | | | | |
| | Set | Cancel | | | | | |
| | | | | | | | |

- 4. Click the **Set** button to save parameters.
- 5. Repeat step 11 14 for extended farms: Server_53_Farm and App_Server_Farm to add Client NAT Address Range.

Configure L7 Persistency for the web farm

Persistence is handled differently for the web tier and the application tier. The application tier accomplishes this through the L7 rules defined earlier in the layer 7 policy tables. The web tier is configured with cookie insertion configured below.

1. From the menu, select **AppDirector** ⇒ **Farms** ⇒ **Extended Parameters** to display the **Extended Farm Parameters** page similar to the one shown.

Extended Farm Parameters								
Farm Table								
Farm Name	Client NAT Address Range	Close Session At Aging	Add X-Forwarded-For to HTTP requests	Insert Cookie for HTTP Persistency	Reset Client on Server Failure			
web server farm	0.0.0.0	Enabled	Disabled	Enable and remove cookie on return path	Disabled			
App_Server_Farm	10.10.10.100	Disabled	Disabled	Disabled	Disabled			
Server_50_Farm	10.10.10.100	Disabled	Disabled	Disabled	Disabled			
Server_53_Farm	10.10.10.100	Disabled	Disabled	Disabled	Disabled			

 Select the "web_server_farm" under the Farm Name to display the Extended Farm Parameters Update page, enter the necessary parameters as shown below:

Extended Farm Parameters Update

Farm Table			
Farm Name:	web server farm	Radius Secret:	
Connection Limit Exception:	Disabled 💌	Client NAT Address Range:	0.0.0.0 -
SSL ID Tracking:	Disabled 💌	Close Session At Aging:	Enabled -
RADIUS Attribute:	0	Reset Client on Server Failure:	Disabled 👻
RADIUS Proxy Attribute:	0	Add X-Forwarded-For to HTTP requests:	Disabled -
Insert Cookie for HTTP Persistency:	Enable and remove cookie on return path -	Hash Parameter For SIP:	Call-ID 👻
SSL ID Aging:	120	Select Server Per Transaction:	Disabled 👻
	Set Can	cel	

3. Click the Set button to save parameters.

Note: Configuring Cookie Insertion for Web Service HTTP Persistence in the Extended Farm Parameters Update page generates all the L7 persistence logic automatically from the single drop down menu. See Appendix 3 to view and better understand the entries that auto generate to facilitate this function.

Layer 7 Persistency – Insert Cookie Settings

When the **Insert Cookie for HTTP Persistency** parameter is enabled in a farm, if the value of this parameter is set to **Enabled**, AppDirector automatically generates a Layer 7 modification rule that inserts a cookie on server replies that contain a server specific identifier. This identifier is used in subsequent requests for Session based persistency. If *Insert Cookie for HTTP Persistency* is set to **"Enable and remove on return path**" AppDirector automatically generates two Layer 7 modification rules, one that inserts a cookie that contains a server specific identifier and one that removes this identifier from subsequent requests before forwarding them to the server. The Layer 7 methods and modification rules that are automatically generated are read-only. If a user deactivates the capability in the farm configuration, the Layer 7 Modification rule and Layer 7 method automatically generated for this capability are removed.

Adding Servers to the Farm

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

Server Table									?		
Farm Table	Physical Se	ervers Static S	ession ID Per	sistency							
Server Name	Farm Name	Server Address	Server Port	Operational Status	Operation Mode	Admin Status	Redirect To	Client NAT	Backup Server Address	Backup Preemption	×
										Delete Cr	eate

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

Server Table Create

Farm Table	Physical S	ervers	Static Session II) Persi	istency		
Farm Name:		Server_	60_Farm) 💌		Server Address:	(10.10.10.50)	
Server Port:		None		*	Server Name:	siebel_server_50	
Server Descript	ion:	siebel_s	erver_50)		Admin Status:	Enable 💌	
Weight:		1			Operation Mode:	Regular 🛩	
Type:		Regular	*		Connection Limit:	0	
Response Thre	shold [ms]:	0			Client NAT:	Enabled 💙	
Backup Server	Address:	0.0.0.0			Redirect To:		
Bandwidth Limi	t:	No Limit		*	Backup Preemption:	Enabled 💌	
Client NAT Add	ress Range:	(10.10.1	0.100 🕶		Farm Name for Local Farm :	None 💌	
			Se	et	Cancel		

- 4. Click the Set button to save parameters.
- 5. On **Server Table** page Click the **Create** button to configure another server. enter the necessary parameters as shown below:

Server Table Create							
Farm Table Physical S	Servers Static Session ID Pers	istency					
Farm Name:	Server_53_Farm	Server Address:	10.10.10.53				
Server Port:	None	Server Name:	siebel_server_53				
Server Description:	siebel_server_53	Admin Status:	Enable 💌				
Weight:	1	Operation Mode:	Regular 💌				
Туре:	Regular 💙	Connection Limit:	0				
Response Threshold [ms]:	0	Client NAT:	Enabled 💙				
Backup Server Address:	0.0.0.0	Redirect To:					
Bandwidth Limit:	No Limit 💌	Backup Preemption:	Enabled 💌				
Client NAT Address Range:	10.10.10.100	Farm Name for Local Farm :	None 💌				
	Set	Cancel					

- 6. Click the **Set** button to save parameters.
- 7. On **Server Table** page Click the **Create** button to configure another server. enter the necessary parameters as shown below:

Server Table Create

Farm Table	Physical S	ervers	Static Se	ssion I	D Persi	stency		
Farm Name:		(web serv	er farm	•		Server Address:	(10.10.10.50	
Server Port:		None			•	Server Name:	web_50	
Server Descriptio	on:	web_50)			Admin Status:	Enable -	
Weight:		1				Operation Mode:	Regular 👻	
Type:		Regular		•		Connection Limit:	0	
Response Threst	hold [ms]:	0				Client NAT:	Disabled 👻	
Backup Server A	ddress:	0.0.0.0	•			Redirect To:		
Bandwidth Limit:		No Limit			•	Backup Preemption:	Enabled -	
Client NAT Addre	ess Range:	0.0.0.0	•			Farm Name for Local Farm :	None -	
				S	et	Cancel		

- 8. Click the **Set** button to save parameters.
- 9. On **Server Table** page Click the **Create** button to configure another server. enter the necessary parameters as shown below:

Farm Table Physical S	Servers Static Session ID Pers	istency		
Farm Name:	web server farm) 🔻	Server Address:	10.10.10.53	
Server Port:	None 🗸	Server Name:	web_53	
Server Description:	web_53	Admin Status:	Enable -	
Weight:	1	Operation Mode:	Regular 👻	
Туре:	Regular -	Connection Limit:	0	
Response Threshold [ms]:	0	Client NAT:	Disabled 👻	
Backup Server Address:	0.0.0.0	Redirect To:		
Bandwidth Limit:	No Limit 🗸	Backup Preemption:	Enabled -	
Client NAT Address Range:	0.0.0.0 -	Farm Name for Local Farm :	None -	
	Set	Cancel		

Server Table Create

- 10. Click the **Set** button to save parameters.
- 11. On **Server Table** page Click the **Create** button to configure another server. enter the necessary parameters as shown below:

Server Table Create

Server Table Create

Farm Table	Physical S	ervers	Static Sessi	on ID Pers	istency		
Farm Name:		App_Se	ver_Farm 👻		Server Address:	(10.10.10.50)	
Server Port:		None		•	Server Name:	(Application_Server_50)	
Server Descript	ion:	Applicati	on_Server_50		Admin Status:	Enable -	
Weight:		1			Operation Mode:	Regular 👻	
Type:		Regular	•		Connection Limit:	0	
Response Three	shold [ms]:	0			Client NAT:	Enabled) -	
Backup Server	Address:	0.0.0.0	•		Redirect To:		
Bandwidth Limi	t:	No Limit		•	Backup Preemption:	Enabled -	
Client NAT Add	ress Range:	(10.10.10	.100) 👻		Farm Name for Local Farm :	None -	
				Set	Cancel		

- 12. Click the **Set** button to save parameters.
- 13. On **Server Table** page Click the **Create** button to configure another server. enter the necessary parameters as shown below

Farm Table Physical	Servers Static Session ID Per	sistency	
Farm Name:	App_Server_Farm) ▼	Server Address:	10.10.10.53
Server Port:	None -	Server Name:	Application_Server_53
Server Description:	Application_Server_53	Admin Status:	Enable -
Weight:	1	Operation Mode:	Regular 🝷
Туре:	Regular 👻	Connection Limit:	0
Response Threshold [ms]:	0	Client NAT:	Enabled) 🗸
Backup Server Address:	0.0.0.0	Redirect To:	
Bandwidth Limit:	No Limit 🗸	Backup Preemption:	Enabled -
Client NAT Address Range	: (10.10.100) -	Farm Name for Local Farm :	None -
	Set	Cancel	

14. Verify that the new entries were created on the Server Table page:

Server Table

Farm Table Physical Servers Static Session ID Persistency

Server Name	Farm Name	Server Address	Server Port	Operational Status	Operation Mode	Admin Status	Redirect To	Client NAT	Backup Server Address	Backup Preemption	×
web_50	web server farm	10.10.10.50	None	Active	Regular	Enable		Disabled	0.0.0	Enabled	
web_53	web server farm	10.10.10.53	None	Active	Regular	Enable		Disabled	0.0.0	Enabled	
Application_Server_50	App_Server_Farm	10.10.10.50	None	Active	Regular	Enable		Enabled	0.0.0.0	Enabled	
Application_Server_53	App_Server_Farm	10.10.10.53	None	Active	Regular	Enable		Enabled	0.0.0.0	Enabled	
siebel_server_50	Server_50_Farm	10.10.10.50	None	Active	Regular	Enable		Enabled	0.0.0	Enabled	
siebel_server_53	Server_53_Farm	10.10.10.53	None	Active	Regular	Enable		Enabled	0.0.0.0	Enabled	
										Delete	Create

Health Monitoring

Create Health Checks

- 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:

Check Table	Binding	Table	HM Server Table			
Health Monitoring Response Level S SSL Certificate E	Status: Samples: ntry Name:	enable) 0 rdwrhm	▼			
Set						

Health Monitoring Global Parameters

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

Health Monitoring Check Table

Binding Table	Pac	ket Sequer	nce Table	Healt	h Monitoring	Global	Para	meters
Check Name		Check ID	Method	Status	Destinatio	n Host	×	
								1
					Delete	Crea	ite	

- 6. Click the **Create** button.
- 7. Create a set of health checks for the web servers. On the **Health Monitoring Check Table Create** page, enter the necessary parameters as shown below:

Health Monitoring Check Table Create								
Binding Table Pa	icket Sequence Table	Health Monitoring Global Par	rameters					
Check Name:	Web_50	Method:	(HTTP) 🔻					
Destination Host:	(10.10.10.50)	Next Hop:	0.0.0.0					
Destination Port:	0	Arguments:	PATH=/iisstart.htm HOST					
Interval:	10	Retries:	5					
Timeout:	5	No New Session Timeout:	0					
Measure Response Tir	me: Disabled 👻	Reverse Check Result:	disable 🔻					
		Set Cancel						

- 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:

Path:	(/iisstart.	htm)				
Hostname:	(10.10.10.50)					
HTTP Method:	GET	•				
Proxy HTTP:	No 👻					
Pragma Nocache:	No 🔻					
Username:						
Password:	1					
Match search string:						
Match mode:						
HTTP return code:	200					
HTTP return code:						
HTTP return code:	ĺ.					
HTTP return code:	1					

- 10. Click the **Set** button for the Method Arguments and click the **Set** button again in the **Health Monitoring Check Table Create** window.
- 11. Follow steps 5-10 to create the second server health check for web server web_53, host 10.10.10.53.
- 12. Create a second set of health checks for the application servers. On the **Health Monitoring Check Table Create** page, enter the necessary parameters as shown below:

Binding Table Pa	acket Sequence Table	Health Monitoring Global Pa	rameters
Check Name:	Sisnapi_HTTP_Broker_	_50) Method:	(HTTP) 🗸
Destination Host:	(10.10.10.50)	Next Hop:	0.0.0.0
Destination Port:	2321	Arguments:	PATH=/SBA_80/SCBroke
Interval:	10	Retries:	5
Timeout:	5	No New Session Timeout:	0
Measure Response Ti	ime: Disabled 🔻	Reverse Check Result:	disable 👻
	s	et Cancel	

Health Monitoring Check Table Create

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

Path:	(SBA_80/SCBroker)
Hostname:	(10.10.10.50)
HTTP Method:	GET 👻
Proxy HTTP:	No 🔻
Pragma Nocache:	No 🔻
Jsemame:	
^D assword:	-
Match search string:	SCBroker Okay
/lat <mark>ch m</mark> ode:	(String exists) 🔹
TTP return code:	
ITTP return code:	
ITTP return code:	
TTP return code:	

Arguments for HTTP Method

- 15. Click the **Set** button for the Method Arguments and click the **Set** button again in the **Health Monitoring Check Table Create** window.
- 16. Follow steps 12-15 to create the second server health check for Application server Application_Server_53, host 10.10.10.53.
- 17. Verify the new entries were created on the Health Monitoring Check Table

Health Monitoring Check Table

Binding Table Packet	Sequence	Table I	Health Monitoring Global Paramet				
Check Name	Check ID	Method	Status	Destination Host	×		
Sisnapi_HTTP_Broker_50	7	HTTP	Passed	10.10.10.50			
Sisnapi_HTTP_Broker_53	1	HTTP	Passed	10.10.10.53			
Web_50	5	HTTP	Passed	10.10.10.50			
Web_53	4	HTTP	Passed	10.10.10.53			
				Delete Crea	ate		

The status of this check may display "Unknown" until the server replies successfully to the AppDirector's check.

Binding Health Checks to Servers

- 1. Create the Health Monitoring Binding for the Servers
- 2. From the menu, select **Health Monitoring** ⇒ **Binding Table** to display the **Health Monitoring Binding Table** page similar to the one shown below:



3. Click the **Create** button.

 Create the health check binding for the web servers. On the Health Monitoring Binding Table Create page, enter the necessary parameters as shown below:

Health M	lonitoring	Binding	lable	Create	

...

Check Table	HM Server Table	Health Monitoring	Global Parameters	
Check: Web_5	0 •	Server/NHR/Report:	(Farm web server farm	- 10.10.10.50 - 0) 🔻
Group: 0		Mandatory:	Mandatory -	
		Set Canc	el	

- 5. Click the **Set** button to save parameters.
- Follow steps 2-5 to bind the second web server health check. Web_53: Farm web server farm - 10.10.10.53 – 0
- 7. Create the health check binding for the application servers. On the **Health Monitoring Binding Table Create** page, enter the necessary parameters as shown below:

Health Monitoring Binding Table Create

Check Table	HM Server Table	Health Monitoring Global Parameters
Check: Sisnap	HTTP_Broker_50	Server/NHR/Report: Farm App_Server_Farm - 10.10.10.50 - 0
Group: 0		Mandatory: Mandatory -
		Set Cancel

- 8. Click the Set button to save parameters.
- Follow steps 7-8 to bind the second application server health check. Sisnapi_HTTP_Broker_53: Farm web server farm - 10.10.10.53 – 0
- 10. Verify that the new entries were created on the **Health Monitoring Binding Table** page:

Health Monitoring Bin	ding la	ble				
Check Table HM Serve	k Table HM Server Table Health Mor					
Check	Server/N	IHR/Report	Group	Mandatory	×	
Sisnapi_HTTP_Broker_53	Farm App_Set 10.10.10	rver_Farm -).53 - 0	0	Mandatory		
<u>Web_53</u>	Farm we farm - 10 - 0	b server 0.10.10.53	0	Mandatory		
<u>Web_50</u>	Farm we farm - 10 - 0	b server 0.10.10.50	0	Mandatory		
Sisnapi_HTTP_Broker_50	Farm App_Set 10.10.10	rver_Farm -).50 - 0	0	Mandatory		
			Delet	e Crea	ate	

This completes the AppDirector Policy Configurations.

General Redundant Configuration Notes

For complete high-availability, Radware encourages implementing pairs of AppDirector units in an Active / Backup configuration. If your implementation of this architecture includes only a single AppDirector, then it is unnecessary to follow the steps in this section.

The overall configuration of a backup AppDirector is almost identical in many ways to that of the active device. There are, however, several important differences that are noted throughout these steps. Radware offers two means of redundancy and failover between pairs of devices – Proprietary and VRRP. Since VRRP is a more commonly used method within the industry, this section will cover the steps to configure both AppDirectors using that method.²

There are separate configuration steps to be taken on both the Active and Backup AppDirector devices, and this section is divided into two parts – one for the active device and one for the backup device.

² For a detailed discussion of VRRP, see RFC 3768.

Follow the steps previously defined to create the Backup AppDirector configuration. The only difference between the primary and the backup device beyond what is yet to be defined specifically for VRRP is the **Redundancy Status** setting. In the Backup AppDirector configuration when configuring the **Layer 4 Policy Table Create** the **Redundancy Status** needs to be set to **Backup** on all farm definitions. The suggested change in configurations instructions is defined below.

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:

Layer 4 Poli	Layer 4 Policy Table										?		
Farm Table	Layer 7 Policy	Fable SS	SL Policy	Table	Cachi	ng Policy Tat	compression of the compression o	ession Policy	Table	Client Authentication	Policy Table	Layer 4 Policy Statistics	
Virtual IP	L4 Policy Name	L4 Protocol	L4 Port	Source From	IP	Source IP To	L7 Policy Name	Farm Name	SSL Policy	Compression Policy	Caching Policy	Client Authentication Policy	×
												Delete Crea	ate

- 2. Click the **Create** button.
- 3. On the **Layer 4 Policy Table Create** page, enter the parameters as on the primary AppDirector with the exception to the Redundancy status, set the status to backup as shown below.

Farm Table Layer / Policy Table SSL Policy Table Caching Policy Table Compression Policy Table Client Authentication Policy Table La L4 Policy Name: WebServiceHTTP Virtual IP: 76.197.19.55 L4 Protocol: TCP TCP <td< th=""><th>Layer 4 Policy Statistic</th></td<>	Layer 4 Policy Statistic
4 Policy Name: WebServiceHTTP Virtual IP: 76.197.19.55 L4 Protocol: TCP APplication: HTTP	
14 Policy Name: WebSeniceHTTP Virtual IP: 76.197.19.55 L4 Protocol: TCP 14 Port: 80 Source IP From: 0.0.0 Application: HTTP Source IP To: 0.0.0 *arm Name: web server farm L7 Policy Name: None ▼ *SL Policy: None Client Authentication Policy: None ▼ *aching Policy: Siebel ▼ Compression Policy: Siebel ▼	
4 Policy Name: WebSeniceHTTP Virtual IP: 76.197.19.55 L4 Protocol: TCP 4 Port: 80 Source IP From: 0.0.0 Application: HTTP Source IP To: 0.0.0 Farm Name: web server farm<	
Virtual IP: 76.197.19.55 L4 Protocol: TCP L4 Port: 80 Source IP From: 0.0.0.0 Application: HTTP Source IP To: 0.0.0 Farm Name: web server farm L7 Policy Name: None SSL Policy: None Client Authentication Policy: None Caching Policy: Siebel	
Virtual IP: 76.197.19.55 L4 Protocol: TCP L4 Port: 80 Source IP From: 0.0.0.0 Application: HTTP	
L4 Port: 80 Source IP From: 0.0.0.0 Application: HTTP Source IP From: 0.0.0.0 Farm Name: web server farm L7 Policy Name: None SSL Policy: None Client Authentication Policy: None Caching Policy: Siebel Compression Policy: Siebel	
Application: HTTP Source IP To: 0.0.0 Farm Name: web server farm L7 Policy Name: None SSL Policy: None Client Authentication Policy: None Caching Policy: Siebel Compression Policy: Siebel	
Farm Name: web server farm It? Policy Name: None SSL Policy: None Client Authentication Policy: None Caching Policy: Siebel Compression Policy: Siebel	
Farm Name: web server farm L7 Policy Name: None SSL Policy: None Client Authentication Policy: None Caching Policy: Siebel Compression Policy: Siebel	
SSL Policy: None • Caching Policy: Siebel • Compression Policy: Siebel •	
Caching Policy: Siebel Compression Policy: Siebel	
POST Classification Input: Header	
Bytes of Request to Read: 3584 HTTP Normalization: Disabled -	
L7 Persistent Switching Mode: Maintain - Policy DefinedBy: User Defined	

- 4. Click the **Set** button to save the parameters.
- 5. Repeat steps 1-4 for each Layer 4 policy.

Primary AppDirector VRRP Configuration

The Virtual Router Redundancy Protocol (VRRP) is designed to eliminate the single point of failure inherent in the static default routed environment. VRRP specifies an election protocol that dynamically assigns responsibility for a virtual router to one of the VRRP routers on a LAN. The VRRP router controlling the IP address(es) associated with a virtual router is called the Master, and forwards packets sent to these IP addresses. The election process provides dynamic fail-over in the forwarding responsibility should the Master become unavailable. Any of the virtual router's IP addresses on a LAN can then be used as the default first hops router by end-hosts.

Global Redundancy Configuration

1. From the menu, select **AppDirector** ⇒ **Redundancy** ⇒ **Global Configuration** and set the parameters as noted below:

IP Redundancy Table	Virtual Rou	iter Table		
			_	
IP Redundancy Admin Stat	us:	(VRRP)	*	
Interface Grouping:	Enabled	*		
ARP With Interface Groupin	ig:	Send 💌		
Backup Device in VLAN:		Disabled	*	
Backup Fake ARP:		Enabled 💌		
Backup Interface Grouping:		(Enabled)	*	
VRRP Advertise Interval [m:	sec]:	0		
VRRP Automated Configura	ation Updates:	Enabled	*	
Force Down Ports Time:		0		
Failure Action:		Ignore	•	
	Set			

Global Redundancy Configuration

2. Click the **Set** button to save these changes.

Primary Virtual Routers

1. From the menu, select **AppDirector** ⇒ **Redundancy** ⇒ **VRRP** ⇒ **Virtual Routers** to display the **Virtual Router Table** page similar to the one shown below. Virtual Router Table

 Global Redundancy Configuration
 Associated IP Addresses
 Active Device Parameters
 Backup Device Parameters
 Mirror Device Parameters

 VRIDs Up/Down: No Change Virtual Router Table
 Virtual Router Table
 Virtual Router Table
 Virtual Router Table

 If Index VR ID
 VR MAC
 State
 Admin Status X
 Virtual Router

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

Virtual Router Table Create										
Global Redun	dancy Configuration	Associated IP Addres	ses Active Device Parameter	Backup Device Parameters	Mirror Device Parameters					
If Index:	G-1 •	VR ID:	1							
Admin Status:	Down 👻	Priority:	255							
Primary IP:	0.0.0.0	Auth Type:	No Authentication 👻							
Auth Key:		Advertise Interval: 1	1							
Preempt Mode:	True 🔻	Protocol: I	lp ▼							
	Set	Cancel								

- 4. Click the **Set** button to save the parameters.
- 5. On the **Virtual Router Table Create** page, click the **Create** button to configure another interface. enter the necessary parameters as shown below:

Virtual Router Table Create										
Global Redun	dancy Configuration	Associated IP Addresses		es Active Device Parameters		Backup Device Par	ameters	Mirror Device Parameters		
If Index:	(G-11) ▼	VR ID:	2]					
Admin Status:	Down 👻	Priority:	255]					
Primary IP:	0.0.0.0	Auth Type:	No Au	thentication 👻						
Auth Key:		Advertise Interval:	1]					
Preempt Mode:	True 🔻	Protocol:	lp ▼							
	Set	Cancel								

- 6. Click the **Set** button to save the parameters.
- 7. Verify that the new entries were created on the Virtual Router Table page:

Virtual Router Table

al F	ledunda	incy Configurat	ion As	sociated IP Add	resses	Active Device Parameters	Backup Device Parameters	Mirror Device Paran
	V	/RIDs Up/Down:	No Chang	e 🔻				
Set								
		Virtual Rout	ter Table					
Index	VR ID	VR MAC	State	Admin Status	×			
<u>-1</u>	1	00005e000101	initialize	Down				
.11	2	00005e000102	initialize	Down				
			De	elete Cre	ate			

Primary Associated IP Addresses

 From the menu, select AppDirector ⇒ Redundancy ⇒ VRRP ⇒ Associated IP Addresses to display the Associated IP Addresses page similar to the one shown below:

Associated IP Addresses				
Global Redundancy Configuration	Virtual Router Table	Active Device Parameters	Backup Device Parameters	Mirror Device Parameters
If Index VR ID Associated IP	٢			
Delete Create				

- 2. Click the **Create** button
- 3. On the **Associated IP Addresses Create** page, enter the necessary parameters as shown below:

Associated IP Addresses Create									
Global Redundancy Configuration	Virtual Router Table	Active Device Parameters	Backup Device Parameters	Mirror Device Parameters					
If Index: G-1 -	VR ID: 1 -								
Associated IP: (76.197.19.61)									
Set Cancel									

- 4. Click the **Set** button to save the parameters
- Follow steps 2-4 to create the associated IP Addresses 76.197.19.55((VIP), VR ID = 1), 10.10.10.1((default gateway for the web servers), VR ID = 2) and 10.10.10.55 ((Application VIP), VR ID = 2).
- 6. Verify that the new entries were created on the **Associated IP Addresses** page:

Associated IP Addresses

 Global Returnation
 Virtual Router Table
 Active Device Parameters
 Backup Device Parameters
 Mirror Device Parameters

 I no 2
 Associated IP
 Image: Constraint of Constraints
 Image: Constraint of Constraints
 Image: Constraints

7. Go to **AppDirector** ⇒ **Redundancy** ⇒ **VRRP** ⇒ **Virtual Routers** and click on the link to If Index <u>G-1</u>

Virtual Router Table										
Global Redundancy Configuration Associated IP Addresses Active Device Parameters Backup Device Parameters Mirror Device Parameters										
VRIDs Up/Down: No Change ▼										
		Virtual Rout	ter Table							
If Index	VR ID	VR MAC	State	Admin Status	\mathbf{X}					
<u>G-1</u>	1	00005e000101	initialize	Down						
<u>G-11</u>	<u>S-11</u> 2 00005e000102 initialize Down									
	Delete Create									

8. Change the **Admin Status** from *down* to *up*, but leave all other settings unchanged:

Virtual Router Table Update

Global Redund	lancy Configuration	Associated IP Addresses		Active Device Pa	rameters	Backup Device Parameters	Mirror Device Parameters
If Index:	G-1	VR ID:	1				
VR MAC:	00005e000101	State:	initial	ize			
Admin Status:	Up 🗸	Priority:	255				
Address Count:	2	Master IP:	0.0.0	.0			
Primary IP:	76.197.19.61	Auth Type:	No Aut	thentication 👻			
Auth Key:		Advertise Interval:	1				
Preempt Mode:	True 💌	Up Time:	0				
Protocol:	lp ▼						
	Set	Cancel					

- 9. Click the Set button to save the parameters.
- 10. Or you can bring all the interfaces up by selecting **VRIDs** to **All Up** click the **Set** button to save the parameters.

Virtual Router Table										
Global I	Redunda	ancy Configurat	ion As	sociated IP Add	esses	Active Device Parameters	Backup Device Parameters	Mirror Device Parameters		
VRIDs Up/Down: All Up										
If Index	VR ID	VR MAC	State	Admin Status	×					
<u>G-1</u>	1	00005e000101	initialize	Down						
<u>G-11</u>	2	00005e000102	initialize	Down						
	Delete Create									

11. Make certain that the **State** of this VR is displayed as *Master* in the Virtual Router table:

Global I	Redunda	ancy Configurati	ion /	Associa	ed IP Ad	dresses	Active Device Parameters	Backup Device Parameters	Mirror Device Parameters	
	VRIDs Up/Down: All Up									
		Virtual Rout	er Table							
If Index	VR ID	VR MAC	State	Adm	n Status	×				
<u>G-1</u>	1	00005e000101	maste	r Up)					
<u>G-11</u>	2	00005e000102	maste	r Up	J					
	Delete Create									

This completes VRRP redundancy configuration on the Active AppDirector.

Backup AppDirector VRRP Configuration

Note: Interface Grouping is not required for the backup AppDirector because of the working assumption that if the Backup device holds Master VRRP status we should continue to provide best effort traffic management even if a single interface is lost.

1. On the Backup AppDirector, go to **AppDirector** ⇒ **Redundancy** ⇒ **Global Configuration** and change the following setting:

Global Redundancy Configuration

IP Redundancy Table	Virtual Rou	iter Table
IP Redundancy Admin Stat	us:	VRRP 🖌
Interface Grouping:		Disabled 🛩
ARP With Interface Groupin	ig:	Send 🛩
Backup Device in VLAN:		Disabled 🛩
Backup Fake ARP:		Enabled 💌
Backup Interface Grouping:		Enabled V
VRRP Advertise Interval [ms	sec]:	0
VRRP Automated Configura	ation Updates:	Enabled 💌
Force Down Ports Time:		0
Failure Action:		Ignore 🗸
	Set	

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

Backup Virtual Routers

3. From the menu, select **AppDirector** ⇒ **Redundancy** ⇒ **VRRP** ⇒ **Virtual Routers** to display the **Virtual Router Table** page similar to the one shown below.

Virtual Router Table									
Global Redundancy Configuration	Associated IP Addresses	Active Device Parameters	Backup Device Parameters	Mirror Device Parameters					
VRIDs Up/Down: No Change									
Virtual Router	Table								
If Index VR ID VR MAC St	ate 🛛 Admin Status 🗙								
	Delete Create								

- 4. Click the **Create** button
- 5. On the **Virtual Router Table** page, enter the necessary parameters as shown below.

Virtual Router Table Create

Global Redun	dancy Configuration	Associated IP Addres	sses Active Device	Parameters	Backup Device Parameters	Mirror Device Parameters
If Index:	G-1 •	VR ID:	1			
Admin Status:	Down 👻	Priority: (100			
Primary IP:	0.0.0.0	Auth Type:	No Authentication	·		
Auth Key:		Advertise Interval:	1			
Preempt Mode:	True 🔻	Protocol:	lp ▼			
	Set	Cancel				

Note: that the Priority on the Backup AppDirector is set to 100 while on the Primary device, this value was set to 255. The device with the higher priority will be Master of this Virtual Router.

- 6. Click the **Set** button to save the parameters.
- On the Virtual Router Table Create page, click the Create button to configure another interface. enter the necessary parameters as shown below:
 Virtual Router Table Create

Global Redun	dancy Configuration	Associated IP Addre	esses Activ	ve Device Para	meters	Backup Device Pa	rameters	Mirror Device Parameters
If Index:	G-11 •	VR ID:	2					
Admin Status:	Down -	Priority:	100					
Primary IP:	0.0.0.0	Auth Type:	No Authentic	ation 🝷				
Auth Key:		Advertise Interval:	1					
Preempt Mode:	True 🔻	Protocol:	lp ▼					
	Set	Cancel						

8. Verify that the new entries were created on the Virtual Router Table page:

Virtual	Virtual Router Table									
Global I	Global Redundancy Configuration Associated IP Addresses Active Device Parameters Backup Device Parameters Mirror Device Parameters									
	VRIDs Up/Down: No Change 👻									
		Set								
		Virtual Rout	ter Table							
If Index	VR ID	VR MAC	State	Admin Statu	s 🗙					
<u>G-1</u>	1	00005e000101	initialize	Down						
<u>G-11</u>	<u>G-11</u> 2 00005e000102 initialize Down									
			D	elete C	eate					

Backup Associated IP Addresses

1. From the menu, select AppDirector ⇒ Redundancy ⇒ VRRP ⇒ Associated IP Addresses to display the Associated IP Addresses Create page similar to the one shown below:

Associated IP Addresses

Associated IP Addresses

Global Redundancy Configuration Virtual Router Table Active Device Parameters Backup Device Parameters Mirror Device Parameters



- 2. Click the **Create** button
- 3. On the **Associated IP Addresses Create** page, enter the necessary parameters as shown below:

Note: This association entry is the interface address of the Primary AppDirector. Since that IP address functions as the default gateway address for each of the farm servers, we will need the backup AppDirector to assume responsibility for this IP if the Active device fails. This is why it is defined in the backup AppDirector's Associated IP Address table. The Association Table from both devices should match when complete.

Associated IP Addresses Crea	te			
Global Redundancy Configuration	Virtual Router Table	Active Device Parameters	Backup Device Parameters	Mirror Device Parameters
If Index: G-1 ▼	VR ID: 1 -			
Associated IP: (76.197.19.61)				
Set Cancel				

- 4. Click the **Set** button to save the parameters
- 5. Follow steps 2-4 to create the associated IP Addresses 76.197.19.55((VIP), VR ID = 1), 10.10.10.1((default gateway for the web servers), VR ID = 2) and 10.10.10.55 ((Application VIP), VR ID = 2).
- 6. Verify that the new entries were created on the **Associated IP Addresses** page:

Global	Redunda	ancy Configurati	on	Virtual Router Table	Active Device Parameters	Backup Device Parameters	Mirror Device Parame
If Index	VR ID	Associated IP	×				
<u>G-1</u>	1	76.197.19.55					
<u>G-1</u>	1	76.197.19.61					
<u>G-11</u>	2	10.10.10.1					
<u>G-11</u>	2	10.10.10.55					
	De	elete Crea	ite				

7. Go to **AppDirector** ⇒ **Redundancy** ⇒ **VRRP** ⇒ **Virtual Routers** and click on the link to If Index <u>G-1</u>

Virtual Router Table Global Redundancy Configuration Associated IP Addresses Active Device Parameters Backup Device Parameters Mirror Device Parameters VRIDs Up/Down: No Change -Set Virtual Router Table If Index VR ID VR MAC State Admin Status G.1 1 00005e000101 initialize Down G.11 2 00005e000102 initialize Down Delete Create

8. Change the **Admin Status** from *down* to *up*, but leave all other settings unchanged:

Virtual Router Table Update

Global Redundancy Configuration Associated IP Addresses Active Device Parameters Backup Device Parameters Mirror Device Parameters

If Index:	G-1	VR ID:	1
VR MAC:	00005e000101	State:	initialize
Admin Status:	Up 🗸	Priority:	255
Address Count:	2	Master IP:	0.0.0.0
Primary IP:	76.197.19.61	Auth Type:	No Authentication -
Auth Key:		Advertise Interval:	1
Preempt Mode:	True 🔻	Up Time:	0
Protocol:	lp ▼		
	Set	Cancel	

- 9. Click the **Set** button to save the parameters.
- 10. Or you can bring all the interfaces up by selecting **VRIDs** to **All Up** click the **Set** button to save the parameters.

Virtual	Virtual Router Table									
Global I	Global Redundancy Configuration Associated IP Addresses Active Device Parameters Backup Device Parameters Mirror Device Parameters									
	VRIDs Up/Down: (All Up) - Set									
		Virtual Rou	ter Table							
If Index	VR ID	VR MAC	State	Admin Status	\times					
<u>G-1</u>	1	00005e000101	initialize	Down						
<u>G-11</u>	2	00005e000102	initialize	Down						
			De	elete Crea	ite					

11. Make certain that the **State** of this VR is displayed as *backup* in the Virtual Router table:

Virtual Router Table

Global F	Redunda	ancy Configurat	ion A	ssociate	d IP Ad	dresses	Active Device Parameters	Backup Device Parameters	Mirror Device Paramet
	V	PIDe Llo/Down	All Lin	-					
	•	Set		-					
		Virtual Rout	er Table						
If Index	VR ID	VR MAC	State	Admir	n Status	×			
<u>G-1</u>	1	00005e000101	backup	Up					
<u>G-11</u>	2	00005e000102	backup	Up					
			De	elete	Cre	ate			

This concludes the configuration of the Backup AppDirector and the local HA solution.

Appendix 1 – Primary AppDirector Configuration File

```
1
!Device Configuration
!Date: 30-12-2008 09:58:49
!DeviceDescription: AppDirector with Cookie Persistency
!Base MAC Address: 00:03:b2:3d:dc:00
!Software Version: 2.00.01 (Build date Nov 20 2008, 09:46:21,Build#9)
!APSolute OS Version: 10.31-03.01A(3):2.06.08
! The following commands will take effect only
! once the device has been rebooted!
system tune bridge-fft-table set 1024
system tune ip-fft-table set 240000
system tune arp-table set 1024
system tune client-table set 1200000
system tune routing-table set 512
system tune url-table set 256
system tune request-table set 5000
system tune nat-address-table set 4
system tune nat-ports-table set 64511
system tune session-id-table set 32000
system tune 13-client-table-size set 20
system tune outbound-nat-address set 1
system tune outbound-nat-ports set 64511
system tune outbound-intrcpt-tbl set 4
system tune radius-attribute-table set 1
system tune segments set 15
system tune 14-policy-table set 512
system tune static-dns-persistency set 5
system tune dynamic-dns-persistency set 10
manage snmp versions-after-reset set "v1 & v2c & v3"
system tune session-pasv-protocols set 16
system tune session set 512
system tune session-resets set 100
! The following commands take effect immediately
! upon execution!
health-monitoring check create Sisnapi_HTTP_Broker_53 -id 1 -m HTTP -p 2321 -a \
"PATH=/SBA_80/SCBroker|HOST=10.10.10.53|MTCH=SCBroker Okay|MEXIST=Y|MTD=G|PR\
X=N|NOCACHE=N|" -d 10.10.10.53
health-monitoring check create Web_53 -id 4 -m HTTP -p 80 -a \
PATH=/iisstart.htm | HOST=10.10.10.53 | MTD=G | PRX=N | NOCACHE=N | C1=200 | -d 10.10.10.53
health-monitoring check create Web_50 -id 5 -m HTTP -p 80 -a \
PATH=/iisstart.htm | HOST=10.10.10.50 | MTD=G | PRX=N | NOCACHE=N | C1=200 | -d 10.10.10.50
health-monitoring check create Sisnapi_HTTP_Broker_50 -id 7 -m HTTP -p 2321 -a \
"PATH=/SBA_80/SCBroker|HOST=10.10.10.50|MTCH=SCBroker Okay|MEXIST=Y|MTD=G|PR\
X=N|NOCACHE=N|" -d 10.10.10.50
net ip-interface create 10.10.10.1 255.255.255.0 11
net ip-interface create 76.197.19.61 255.255.255.240 1
net ip-interface create 192.168.1.50 255.255.255.0 18
net route table create 0.0.0.0 0.0.0.0 76.197.19.62 -i 1
redundancy mode set VRRP
appdirector farm table setCreate "web server farm" -as Enabled -at 7300 \backslash
-dm Cyclic -cm "No Checks" -sm RemoveOnSessionEnd-SPS
appdirector farm table setCreate App_Server_Farm -as Enabled -at 7300 -dm \
Cyclic -cm "No Checks" -sm ServerPerSession
appdirector farm table setCreate Server_50_Farm -as Enabled -at 7300 -dm Cyclic
appdirector farm table setCreate "Server_53_Farm " -as Enabled -at 7300 -dm Cyclic
appdirector farm server table create "web server farm" 10.10.10.50 None -sn web_50 -id 0
appdirector farm server table create "web server farm" 10.10.10.53 None -sn web_53 -id 1
appdirector farm server table create App_Server_Farm 10.10.10.50 None -sn \
Application_Server_50 -id 13 -cn Enabled -nr 10.10.10.100
```

appdirector farm server table create <code>App_Server_Farm 10.10.10.53</code> None <code>-sn $\$ </code> Application_Server_53 -id 14 -cn Enabled -nr 10.10.10.100 appdirector farm server table create Server_50_Farm 10.10.10.50 None -sn $\$ siebel_server_50 -id 19 -cn Enabled -sd siebel_server_50 -nr 10.10.10.100 appdirector farm server table create "Server_53_Farm " 10.10.10.53 None \ -sn siebel_server_53 -id 18 -cn Enabled -sd siebel_server_53 -nr 10.10.10.100 appdirector 17 farm-selection method-table setCreate AppSrv50 -cm \ "Regular Expression" -ma EXP=.*/!5.* appdirector 17 farm-selection method-table setCreate LBAppSrv -cm \ "Regular Expression" -ma EXP=.*| appdirector 17 farm-selection method-table setCreate AppSrv53 -cm \ "Regular Expression" -ma EXP=.*/!1.*| appdirector 17 farm-selection method-table setCreate RR -cm \ "Regular Expression" -ma EXP=.*/RR*| appdirector 17 farm-selection method-table setCreate\ "Auto-G Cookie web s" -cm "Set Cookie" -ma \ KEY=yI8cugcRkX | VAL=\$Server_SID_Cookie | appdirector 17 farm-selection method-table setCreate "Auto-G RCookie web " -cm Cookie -ma KEY=yI8cugcRkX| appdirector 17 farm-selection policy-table setCreate App_lb 10 -m1 \ LBAppSrv -pa PRSST=On | -fn App_Server_Farm appdirector 17 farm-selection policy-table setCreate App_lb 7 -m1 \ AppSrv50 -pa PRSST=On | -fn Server_50_Farm appdirector 17 farm-selection policy-table setCreate App_lb 5 -m1 \ AppSrv53 -pa PRSST=On | -fn "Server_53_Farm " appdirector 17 farm-selection policy-table setCreate App_lb 1 -ml RR -pa \ PRSST=On -fn App_Server_Farm redundancy interface-group set Enabled appdirector dns status set Disabled appdirector nat server status set enable appdirector dns two-records set Disabled redundancy backup-in-vlan set Disabled appdirector farm connectivity-check httpcode setCreate "web server farm" "200 - OK" appdirector farm connectivity-check httpcode setCreate App_Server_Farm "200 - OK" appdirector farm connectivity-check httpcode setCreate Server_50_Farm "200 - OK" appdirector farm connectivity-check httpcode setCreate "Server_53_Farm " "200 - OK" appdirector 17 server-persistency static-persist-table setCreate\ "web server farm" narXaheDdlFn -sa 10.10.10.50 -sp 0 -fl 1 appdirector 17 server-persistency static-persist-table setCreate\ "web server farm" ihtJZ7oCXWeM -sa 10.10.10.53 -sp 0 -fl 1 appdirector nat server specific-nat-address set 0.0.0.0 redundancy backup-fake-arp set Enabled net next-hop-router setCreate 76.197.19.62 -id 10 -fl 1 appdirector farm nhr setCreate 0.0.0.0 -ip 76.197.19.62 -fl 1 appdirector farm extended-params set App_Server_Farm -nr 10.10.10.100 appdirector farm extended-params set "web server farm" -sc Enabled -ic \setminus "Enable and remove cookie on return path" appdirector farm extended-params set Server_50_Farm -nr 10.10.10.100 appdirector farm extended-params set "Server_53_Farm " -nr 10.10.10.100 appdirector nat client address-range setCreate 10.10.10.100 -t 10.10.10.100 appdirector nat client range-to-nat setCreate 10.10.10.50 -t 10.10.10.53 appdirector nat client status set Enabled redundancy backup-interface-group set Enabled system internal appdirector full-session-id-table setCreate\ "web server farm" 0 TCP -k yI8cugcRkX -fl 1 appdirector nat outbound status set Disabled appdirector 14-policy ssl-policy create Siebel -c SiebelCert -r Enabled appdirector 14-policy compression create Siebel -pe Hardware appdirector 14-policy caching create Siebel appdirector 14-policy table create 76.197.19.53 Any Any 0.0.0.0 Siebel_Server_53 -fn "Server_53_Farm appdirector 14-policy table create 76.197.19.50 Any Any 0.0.0.0 $\$ Siebel_Server_50 -fn Server_50_Farm appdirector 14-policy table create 10.10.10.55 TCP 2321 0.0.0.0 $\$ App_svr_17 -po App_lb -ta HTTP appdirector 14-policy table create 76.197.19.55 TCP 80 0.0.0.0 $\$ WebServiceHTTP -fn "web server farm" -ta HTTP -pm Maintain -co Siebel -ca Siebel redundancy vrrp automated-config-update set Enabled appdirector 17 modification table setCreate "Auto-G Cookie web s" -i 0 -f \ "web server farm" -d Reply -am "Auto-G Cookie web s" appdirector 17 modification table setCreate "Auto-G RCookie web " -i 0 -f \backslash "web server farm" -ac Remove -mm "Auto-G RCookie web "

```
redundancy global-configuration failure-action set Ignore
health-monitoring binding create 1 14
health-monitoring binding create 5 0
health-monitoring binding create 4 1
health-monitoring binding create 7 13
health-monitoring status set enable
health-monitoring response-level-samples set 0
redundancy vrrp virtual-routers create 1 1 -as Up -p 255 -pip 76.197.19.61
redundancy vrrp virtual-routers create 11 2 -as Up -p 255 -pip 10.10.10.1
redundancy vrrp associated-ip create 1 1 76.197.19.61
redundancy vrrp associated-ip create 1 1 76.197.19.55
redundancy vrrp associated-ip create 11 2 10.10.10.1
redundancy vrrp associated-ip create 11 2 10.10.10.55
manage user table create radware -pw GndridF04zNWSGOrZjKFV78REiEra/Qm
manage telnet status set enable
manage telnet server-port set 23
manage web status set enable
manage ssh status set enable
manage secure-web status set enable
services dns client primary-server set 68.94.156.1
services dns client alt-server set 0.0.0.0
services dns client status set Enabled
manage ftp server-port set 21
manage ftp status set enable
redundancy arp-interface-group set Send
net 12-interface set 100001 -ad up
net 12-interface set 100063 -ad up
redundancy vrrp global-advertise-int set 0
manage snmp groups create SNMPv1 public -gn initial
manage snmp groups create SNMPv1 ReadOnlySecurity -gn InitialReadOnly
manage snmp groups create SNMPv2c public -gn initial
manage snmp groups create SNMPv2c ReadOnlySecurity -gn InitialReadOnly
manage snmp groups create UserBased radware -gn initial
manage snmp groups create UserBased ReadOnlySecurity -gn InitialReadOnly
manage snmp access create initial SNMPv1 noAuthNoPriv -rvn iso -wvn iso -nvn iso
manage snmp access create InitialReadOnly SNMPv1 noAuthNoPriv -rvn ReadOnlyView
manage snmp access create initial SNMPv2c noAuthNoPriv -rvn iso -wvn iso -nvn iso
manage snmp access create InitialReadOnly SNMPv2c noAuthNoPriv -rvn ReadOnlyView
manage snmp access create initial UserBased authPriv -rvn iso -wvn iso -nvn iso
manage snmp access create InitialReadOnly UserBased authPriv -rvn ReadOnlyView
manage snmp views create iso 1
manage snmp views create ReadOnlyView 1
manage snmp views create ReadOnlyView 1.3.6.1.4.1.89.2.7.2 -cm excluded
manage snmp views create ReadOnlyView 1.3.6.1.6.3.18.1.1 -cm excluded
manage snmp views create ReadOnlyView 1.3.6.1.6.3.15.1.2.2 -cm excluded
manage snmp views create ReadOnlyView 1.3.6.1.4.1.89.35.1.61 -cm excluded
manage snmp views create ReadOnlyView 1.3.6.1.6.3.16.1.2 -cm excluded
manage snmp views create ReadOnlyView 1.3.6.1.6.3.16.1.4 -cm excluded
manage snmp views create ReadOnlyView 1.3.6.1.6.3.16.1.5 -cm excluded
manage snmp notify create allTraps -ta v3Traps
manage snmp users create radware -cf 0.0 -ap MD5 -akc \backslash
54118f8ecffedac7e39d16b7c9cab095 -pp DES -pkc \
54118f8ecffedac7e39d16b7c9cab095
manage snmp target-address create v3MngStations -tl v3Traps -p radware-authPriv
manage snmp target-parameters create public-v1 -d SNMPv1 -sm SNMPv1 -sn \
public -sl noAuthNoPriv
manage snmp target-parameters create public-v2 -d SNMPv2c -sm SNMPv2c -sn \backslash
public -sl noAuthNoPriv
manage snmp target-parameters create radware-authPriv -d SNMPv3 -sm \
UserBased -sn radware -sl authPriv
manage snmp community create public -n public -sn public
services auditing status set enable
manage telnet session-timeout set 5
manage telnet auth-timeout set 30
system diagnostics policies setCreate Login -i 2 -tr Disabled
system diagnostics capture output file set "ram drive"
system diagnostics capture output term set Disabled
system diagnostics trace-log output file set "ram drive and flash"
system diagnostics trace-log output term set Disabled
system diagnostics trace-log output syslog set Disabled
system diagnostics trace-log modules set HMM -st Enabled -sev Info
system diagnostics capture point set both
```

redundancy force-down-ports-time set 0 system diagnostics capture traffic-match-mode set "Inbound and Outbound" appdirector global connectivity-check tcp-timeout set 3

!File Signature: ab39d5c111a713a32ce4188c4efccef6

Appendix 2 – Backup AppDirector Configuration File

```
!
!Device Configuration
!Date: 31-12-2008 22:08:17
!DeviceDescription: AppDirector with Cookie Persistency
!Base MAC Address: 00:03:b2:4b:16:40
!Software Version: 2.00.01 (Build date Nov 20 2008, 09:46:21,Build#9)
!APSolute OS Version: 10.31-03.01A(3):2.06.08
1
! The following commands will take effect only
! once the device has been rebooted!
1
system tune bridge-fft-table set 1024
system tune ip-fft-table set 240000
system tune arp-table set 1024
system tune client-table set 1200000
system tune routing-table set 512
system tune url-table set 256
system tune request-table set 5000
system tune nat-address-table set 4
system tune nat-ports-table set 64511
system tune session-id-table set 32000
system tune 13-client-table-size set 20
system tune outbound-nat-address set 1
system tune outbound-nat-ports set 64511
system tune outbound-intrcpt-tbl set 4
system tune radius-attribute-table set 1
system tune segments set 15
system tune 14-policy-table set 512
system tune static-dns-persistency set 5
system tune dynamic-dns-persistency set 10
manage snmp versions-after-reset set "v1 & v2c & v3"
system tune session-pasv-protocols set 16
system tune session set 512
system tune session-resets set 100
! The following commands take effect immediately
! upon execution!
1
health-monitoring check create Sisnapi_HTTP_Broker_53 -id 1 -m HTTP -p 2321 -a \
"PATH=/SBA_80/SCBroker|HOST=10.10.10.53|MTCH=SCBroker Okay|MEXIST=Y|MTD=G|PR\
X=N | NOCACHE=N | " -d 10.10.10.53
health-monitoring check create Web_53 -id 4 -m HTTP -p 80 -a \
PATH=/iisstart.htm |HOST=10.10.10.53 |MTD=G |PRX=N |NOCACHE=N |C1=200 | -d 10.10.10.53
health-monitoring check create Web_50 -id 5 -m HTTP -p 80 -a \
PATH=/iisstart.htm |HOST=10.10.10.50 |MTD=G |PRX=N |NOCACHE=N |C1=200 | -d 10.10.10.50
health-monitoring check create Sisnapi_HTTP_Broker_50 -id 7 -m HTTP -p 2321 -a \
"PATH=/SBA_80/SCBroker|HOST=10.10.10.50|MTCH=SCBroker Okay|MEXIST=Y|MTD=G|PR\
X=N|NOCACHE=N|" -d 10.10.10.50
net ip-interface create 192.168.1.53 255.255.255.0 17
net ip-interface create 10.10.10.3 255.255.255.0 11
net ip-interface create 76.197.19.60 255.255.255.240 1
net route table create 0.0.0.0 0.0.0.0 76.197.19.62 -i 1
redundancy mode set VRRP
appdirector farm table setCreate "web server farm" -as Enabled -at 7300 \
-dm Cyclic -cm "No Checks" -sm RemoveOnSessionEnd-SPS
appdirector farm table setCreate App_Server_Farm -as Enabled -at 7300 -dm \
```

Cyclic -cm "No Checks" -sm ServerPerSession appdirector farm table setCreate Server_50_Farm -as Enabled -at 7300 -dm Cyclic appdirector farm table setCreate "Server_53_Farm " -as Enabled -at 7300 -dm Cyclic appdirector farm server table create "web server farm" 10.10.10.50 None -sn web_50 -id 0 appdirector farm server table create "web server farm" 10.10.10.53 None -sn web_53 -id 1 appdirector farm server table create App_Server_Farm 10.10.10.50 None -sn \ Application_Server_50 -id 13 -cn Enabled -nr 10.10.10.100 appdirector farm server table create App_Server_Farm 10.10.10.53 None -sn \backslash Application_Server_53 -id 14 -cn Enabled -nr 10.10.10.100 appdirector farm server table create Server_50_Farm 10.10.10.50 None -sn $\$ siebel_server_50 -id 19 -cn Enabled -sd siebel_server_50 -nr 10.10.10.10.
appdirector farm server table create "Server_53_Farm " 10.10.10.53 None \ -sn siebel_server_53 -id 18 -cn Enabled -sd siebel_server_53 -nr 10.10.10.100 appdirector 17 farm-selection method-table setCreate AppSrv50 -cm \ "Regular Expression" -ma EXP=.*/!5.*| appdirector 17 farm-selection method-table setCreate LBAppSrv -cm \ "Regular Expression" -ma EXP=.*| appdirector 17 farm-selection method-table setCreate AppSrv53 -cm \setminus "Regular Expression" -ma EXP=.*/!1.* appdirector 17 farm-selection method-table setCreate RR -cm \ "Regular Expression" -ma EXP=.*/RR*| appdirector 17 farm-selection method-table setCreate\ "Auto-G Cookie web s" -cm "Set Cookie" -ma \ KEY=yI8cugcRkX | VAL=\$Server_SID_Cookie | appdirector 17 farm-selection method-table setCreate "Auto-G RCookie web " -cm Cookie -ma KEY=yI8cugcRkX| appdirector 17 farm-selection policy-table setCreate App_lb 10 -m1 \ LBAppSrv -pa PRSST=On| -fn App_Server_Farm appdirector 17 farm-selection policy-table setCreate App_lb 7 -ml $\$ AppSrv50 -pa PRSST=On | -fn Server_50_Farm appdirector 17 farm-selection policy-table setCreate App_lb 5 -m1 \ AppSrv53 -pa PRSST=On -fn "Server_53_Farm appdirector 17 farm-selection policy-table setCreate App_lb 1 -m1 RR -pa \ PRSST=On | - fn App_Server_Farm redundancy interface-group set Enabled appdirector dns status set Disabled appdirector nat server status set enable appdirector dns two-records set Disabled redundancy backup-in-vlan set Disabled appdirector farm connectivity-check httpcode setCreate "web server farm" "200 - OK" appdirector farm connectivity-check httpcode setCreate App_Server_Farm "200 - OK" appdirector farm connectivity-check httpcode setCreate Server_50_Farm "200 - OK" appdirector farm connectivity-check httpcode setCreate "Server_53_Farm " "200 - OK" appdirector 17 server-persistency static-persist-table setCreate\ "web server farm" narXaheDdlFn -sa 10.10.10.50 -sp 0 -fl 0 appdirector 17 server-persistency static-persist-table setCreate\ "web server farm" ihtJZ7oCXWeM -sa 10.10.10.53 -sp 0 -fl 0 appdirector nat server specific-nat-address set 0.0.0.0 redundancy backup-fake-arp set Enabled net next-hop-router setCreate 76.197.19.62 -id 20 -fl 1 appdirector farm nhr setCreate 0.0.0.0 -ip 76.197.19.62 -fl 1 appdirector farm extended-params set App_Server_Farm -nr 10.10.10.100 appdirector farm extended-params set "web server farm" -sc Enabled -ic \setminus "Enable and remove cookie on return path" appdirector farm extended-params set Server_50_Farm -nr 10.10.10.100 appdirector farm extended-params set "Server_53_Farm " -nr 10.10.10.100 appdirector nat client address-range setCreate 10.10.10.100 -t 10.10.10.100 appdirector nat client range-to-nat setCreate 10.10.10.50 -t 10.10.10.53 appdirector nat client status set Enabled redundancy backup-interface-group set Enabled system internal appdirector full-session-id-table setCreate\ "web server farm" 0 TCP -k yI8cugcRkX -fl 0 appdirector nat outbound status set Disabled appdirector 14-policy ssl-policy create Siebel -c SiebelCert -r Enabled appdirector 14-policy compression create Siebel -pe Hardware appdirector 14-policy caching create Siebel appdirector 14-policy table create 76.197.19.53 Any Any 0.0.0.0 $\$ Siebel_Server_53 -fn "Server_53_Farm " -rs Backup appdirector 14-policy table create 76.197.19.50 Any Any 0.0.0.0 Siebel_Server_50 -fn Server_50_Farm -rs Backup appdirector 14-policy table create 10.10.10.55 TCP 2321 0.0.0.0 $\$ App_svr_17 -po App_lb -ta HTTP -rs Backup

```
appdirector 14-policy table create 76.197.19.55 TCP 80 0.0.0.0 \
 WebServiceHTTP -fn "web server farm" -ta HTTP -rs Backup -pm Maintain -co \
Siebel -ca Siebel
redundancy vrrp automated-config-update set Enabled
appdirector 17 modification table setCreate "Auto-G Cookie web s" -i 0 -f \
'web server farm" -d Reply -am "Auto-G Cookie web s"
redundancy global-configuration failure-action set Ignore
health-monitoring binding create 1 14
health-monitoring binding create 5 0
health-monitoring binding create 4 1
health-monitoring binding create 7 13
health-monitoring status set enable
health-monitoring response-level-samples set 0
redundancy vrrp virtual-routers create 1 1 -pip 76.197.19.60
redundancy vrrp virtual-routers create 11 2 -pip 10.10.10.3
redundancy vrrp associated-ip create 1 1 76.197.19.61
redundancy vrrp associated-ip create 1 1 76.197.19.55
redundancy vrrp associated-ip create 11 2 10.10.10.1
redundancy vrrp associated-ip create 11 2 10.10.10.55
manage user table create radware -pw GndridF04zNWSGOrZjKFV78REiEra/Qm
manage telnet status set enable
manage telnet server-port set 23
manage web status set enable
manage ssh status set enable
manage secure-web status set enable
services dns client primary-server set 68.94.156.1
services dns client alt-server set 0.0.0.0
services dns client status set Enabled
manage ftp server-port set 21
manage ftp status set enable
redundancy arp-interface-group set Send
net 12-interface set 100001 -ad up
net 12-interface set 100063 -ad up
redundancy vrrp global-advertise-int set 0
manage snmp groups create SNMPv1 public -gn initial
manage snmp groups create SNMPv1 ReadOnlySecurity -gn InitialReadOnly
manage snmp groups create SNMPv2c public -gn initial
manage snmp groups create SNMPv2c ReadOnlySecurity -gn InitialReadOnly
manage snmp groups create UserBased radware -gn initial
manage snmp groups create UserBased ReadOnlySecurity -gn InitialReadOnly
manage snmp access create initial SNMPv1 noAuthNoPriv -rvn iso -wvn iso -nvn iso
manage snmp access create InitialReadOnly SNMPv1 noAuthNoPriv -rvn ReadOnlyView
manage snmp access create initial SNMPv2c noAuthNoPriv -rvn iso -wvn iso -nvn iso
manage snmp access create InitialReadOnly SNMPv2c noAuthNoPriv -rvn ReadOnlyView
manage snmp access create initial UserBased authPriv -rvn iso -wvn iso -nvn iso
manage snmp access create InitialReadOnly UserBased authPriv -rvn ReadOnlyView
manage snmp views create iso 1
manage snmp views create ReadOnlyView 1
manage snmp views create ReadOnlyView 1.3.6.1.4.1.89.2.7.2 -cm excluded
manage snmp views create ReadOnlyView 1.3.6.1.6.3.18.1.1 -cm excluded
manage snmp views create ReadOnlyView 1.3.6.1.6.3.15.1.2.2 -cm excluded
manage snmp views create ReadOnlyView 1.3.6.1.4.1.89.35.1.61 -cm excluded
manage snmp views create ReadOnlyView 1.3.6.1.6.3.16.1.2 -cm excluded
manage snmp views create ReadOnlyView 1.3.6.1.6.3.16.1.4 -cm excluded
manage snmp views create ReadOnlyView 1.3.6.1.6.3.16.1.5 -cm excluded
manage snmp notify create allTraps -ta v3Traps
manage snmp users create radware -cf 0.0 -ap MD5 -akc \backslash
54118f8ecffedac7e39d16b7c9cab095 -pp DES -pkc \
54118f8ecffedac7e39d16b7c9cab095
manage snmp target-address create v3MngStations -tl v3Traps -p radware-authPriv
manage snmp target-parameters create public-v1 -d SNMPv1 -sm SNMPv1 -sn \
public -sl noAuthNoPriv
manage snmp target-parameters create public-v2 -d SNMPv2c -sm SNMPv2c -sn \
public -sl noAuthNoPriv
manage snmp target-parameters create radware-authPriv -d SNMPv3 -sm \backslash
UserBased -sn radware -sl authPriv
manage snmp community create public -n public -sn public
services auditing status set enable
manage telnet session-timeout set 5
manage telnet auth-timeout set 30
system diagnostics policies setCreate Login -i 2 -tr Disabled
system diagnostics capture output file set "ram drive"
```

system	diagnostics	capture output term set Disabled
system	diagnostics	trace-log output file set "ram drive and flash"
system	diagnostics	trace-log output term set Disabled
system	diagnostics	trace-log output syslog set Disabled
system	diagnostics	trace-log modules set HMM -st Enabled -sev Info
system	diagnostics	capture point set both
redunda	ancy force-do	own-ports-time set 0
system	diagnostics	capture traffic-match-mode set "Inbound and Outbound"
appdire	ector global	connectivity-check tcp-timeout set 3

!File Signature: c2f60b9aed3a4f2ab689fdd07ad0b778

Appendix 3 – Insert Cookie - Auto Generated Configuration

Below are the entries that get generated by enabling insert cookie.

From the menu, select **AppDirector** ⇒ **Layer 7 Farm Selection** ⇒ **Methods** to display the **Methods Table** page similar to the one shown below:

Method Table

Layer 7 Policy Table	Layer 7 Policy Sta	tistics Layer 7 Modification Table	
Method Name	Method Type	Arguments	×
AppSrv50	Regular Expression	EXP=.*/!5.*	
AppSrv53	Regular Expression	EXP=.*/!1.*	
Auto-G Cookie web s	Set Cookie	KEY=yl8cugcRkX VAL=\$Server_SID_Cookie	
Auto-G RCookie web	Cookie	KEY=yl8cugcRkX	
LBAppSrv	Regular Expression	EXP=.*	
RR	Regular Expression	EXP=.*/RR*	
		Delete Crea	ite

Select "Auto-G Cookie web s" from the Method Table to display the Methods Table Update page similar to the one shown.

Method Table Update

	iley Table	e Luyer / Por	icy statistics	Layerri	
lethod Nam	ie: Auto	o-G Cookie web s	Me	thod Type:	Set Cookie
rguments:	KEY=	vl8cugcRkX VAL:	=\$\$		
		Set	Cancel		
elect	to see	the Argumen	ts values.		
elect	to see	the Argumen Cookie Method	ts values.		
elect	to see for Set (yl8cugcF	the Argumen Cookie Method RkX	ts values.		
elect Arguments Sey: 'alue:	to see for Set (yl8cugcF \$Server_	the Argumen Cookie Method RkX SID_Cookie	ts values.		
elect Arguments Gey: 'alue: 'ath:	to see for Set (yl8cugcF \$Server_	the Argumen Cookie Method RkX SID_Cookie	ts values.		
elect Arguments Gey: Value: Vath: Iomain:	to see for Set (yl8cugcF \$Server_	the Argumen Cookie Method RkX SID_Cookie	ts values.		

Select "Auto-G RCookie web" from the Method Table to display the Methods Table Update page similar to the one shown.

Method Table Update

Layer 7 Policy	y Table	Layer 7 Policy	Statistics	Layer 7 Mo	dification Table
Method Name:	Auto-G	RCookie web	Me	thod Type: C	ookie -
Arguments:	KEY=yl8	cugcRkX			
		Set	Cancel		

Select		to see	the A	rgun	nents	values.
Argu	ments f	or Cook	ie Met	hod		
Key:	yl8cug	cRkX				

Cancel

Value:

Set

From the menu, select **AppDirector** ⇒ **Layer 7 Modification** ⇒ **Rules** to display the **Layer 7 Modification Table** page similar to the one shown below:

Layer 7 Modification Table

Method Table	od Table Layer 7 Modification Statistics Table					ation	Reset Stati
Name		Farm Name	Index	Admin Status	Direction	×	
Auto-G Cookie w	eb s	web server farm	0	Enabled	Reply		
Auto-G RCookie	web	web server farm	0	Enabled	Request		
				Delete	Сгеа	ate	

Select "Auto-G Cookie web s" from the Layer 7 Modification Table to display the Layer 7 Modification Table Update page similar to the one shown.

Layer 7 Modification Table Update

Method Table	Layer 7 Modification	Statistics Table	Layer 7 Modification Reset Statistics
Name:	Auto-G Cookie web s	Index:	0
Farm Name:	web server farm 🛛 👻	Action:	Insert -
Direction:	Reply -	Match Method:	
Action Method:	Auto-G Cookie web s 👻	Admin Status:	Enabled -
	Set	Cancel	

Select "Auto-G RCookie web" from the Layer 7 Modification Table to display

the Layer 7 Modification Table Update page similar to the one shown.

Layer 7 Modification Table Update								
Method Table	Layer 7 Modification	Statistics Table	Layer 7 Modification Reset Statistics					
Name:	Auto-G RCookie web	Index:	0					
Farm Name:	web server farm 🔹	Action:	Remove -					
Direction:	Request 👻	Match Method:	Auto-G RCookie web 🔻					
Action Method:	-	Admin Status:	Enabled -					
	Set	Cancel						

From the menu, select **AppDirector** ⇒ **Layer 7 Server Persistence** ⇒ **Text Match** to display the **Text Match Session ID Persistence** page similar to the one shown below:

Text Match Session ID Persistency

Pattern Match Se	ession ID Persisten	cy Static S	ession ID Persistency	Farm Table	
Farm Name	Application Port	L4 Protocol	Persistency Identifier	Learning Direction	×
web server farm	0	TCP	yl8cugcRkX	Server Reply	
				Delete Crea	ate

Select "web server farm" from the Text Match Session ID Persistence to display the Text Match Session ID Persistence Update page similar to the one shown.

Pattern Match Se	ssion ID Persistency	Static Session ID Persis	Farm Table	
Farm Name:	web server farm	Application Port:	0	
L4 Protocol:	TCP	Persistency Identifier:	yl8cug	cRkX
Lookup Mode:	Cookie -	Identifier Match:	Exact	•
Learning Direction:	Server Reply -	Ignore Server Reply:	Never	
Value Max Length:	256	Value Offset:	0	
Stop Chars:		Inactivity Timeout:	60	
Ignore Source IP:	Enabled -			
	Set	Cancel		

Text Match Session ID Persistency Update

From the menu, select **AppDirector** ⇒ **Layer 7 Server Persistence** ⇒ **Static Session ID Persistency** to display the **Static Session ID Persistency** page similar to the one shown below:

Static Session ID Persistency

Text Match Sessi	on ID Persistency	Pattern Match	Pattern Match Session ID Persistency			Server Table
Session ID Value	Farm Name	Server Address	Server Port	Value Type	× .	
ihtJZ7oCXWeM	web server farm	10.10.10.53	0	Text		
<u>narXaheDdIFn</u>	web server farm	10.10.10.50	0	Text		
Delete Create						

Select "ihtJZ7oCXWeM" from the Static Session ID Persistency page to display the Static Session ID Persistency Update page similar to the one shown.

Static Session ID Persistency Update

Text Match Session ID Persistency Pattern Mate		h Session ID Persistency	Farm Table	Server Table	
Farm Name:	web server farm Ses	sion ID Value:	ihtJZ7oCXWeM		
Server Address:	10.10.10.53 - Ser	/er Port:	0 👻		
Value Type:	Text -				
	Set Ca	ancel			

Select "narXaheDdIFn" from the Static Session ID Persistency page to display the Static Session ID Persistency Update page similar to the one shown.

Static Session ID Persistency Update								
Text Match Session ID Persistency Pattern Match Session ID Persistency Farm Table Server Table								
Farm Name:	web server farm Ses	sion ID Value: narXaheDdlFn						
Server Address:	10.10.10.50 - Sen	ver Port: 0 👻						
Value Type: Text -								
	Set Ca	ncel						

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

© 2008 Radware, Ltd. All Rights Reserved. Radware and all other Radware product and service names are registered trademarks or trademarks of Radware in the U.S. and other countries. All other trademarks and names are the property of their respective owners.