TESTING & INTEGRATION GROUP

TECHNICAL DOCUMENT

Radware AppDirector with BEA WebLogic Network Gatekeeper (WLNG)

INTRODUCTION……..2
SOLUTION DETAILS……..4
HOW IT WORKS……..5
SOFTWARE AND HARDWARE……..6
NETWORK DIAGRAM……..7
CONFIGURATION……..8
TECHNICAL SUPPORT……..12

TECHNICAL DOCUMENT
AUTHOR: Michael Geigenscheder
DATE: Mai, 2008
Version: 1.2

Introduction

BEA WebLogic Network Gatekeeper delivers an integrated SDP-IMS services layer platform that combines powerful policy enforcement, comprehensive Telecom Web Services, partner relationship management, and an extensible network plug-in framework.

BEA WebLogic Network Gatekeeper provides a secure common entry point for applications accessing network resources both through Telecom Web Services interfaces to service providers and their applications, and through policy-based, secure, and extensible network interfaces. It also accelerates development of new communication applications by abstracting core network resources residing in wireless, wireline, or IP networks, and exposing them to the wider community of IT application developers using industry-standard Web services and Java interfaces, and Telecom Web Services.

The “northbound” application interface layer of BEA WebLogic Network Gatekeeper provides a standardsbased Web services interface to telecom network service capabilities based on a common access control, security, and policy management framework. With the Extension Toolkit, network operators can add network service API extensions. The application interface layer supports APIs based on Parlay X 2.1 and Extended Web Services. BEA WebLogic Network Gatekeeper exposes the following service capabilities as Telecom Web Services

- Call control (Parlay X 2.1/ES 202 391 v1.2.1): third-party call control, call notification, call handling, and audio call
- Messaging (Parlay X 2.1/ES 202 391 v1.2.1): SMS, MMS, and EWS WAP Push (WAP 1.2)
- Mobility (Parlay X 2.1/ES 202 391 v1.2.1): terminal status, terminal location
- Payment (Parlay X 2.1/ES 202 391 v1.2.1)
- Presence (Parlay X 2.1/ES 202 391 v1.2.1).

BEA recommends WebLogic clustering as a solution for scalability and availability, but recognizes the need for an application delivery solution such as the Radware AppDirector (AD) in order to improve performance and fault tolerance through the advantage of offloading the application servers from the task of server load balancing.

Using Radware solutions, maximum application availability can be obtained by using the following:

Advanced health monitoring

Each product of the APSolute product suite has an advanced module of health monitoring which includes an extensive library of pre-defined health checks. By using these checks AppDirector can be set to identify any type of failure, whether it is a server hardware failure, an operating system problem, a specific application failure or a back end database failure.

Load balancing and persistency

Through a wide set of load balancing algorithms, AppDirector optimizes server performance by redirecting users to the least loaded and best performing server thus ensuring the fastest response time to users. Within a BEA environment, AppDirector can optimize the performance of the WebLogic application server farm while ensuring users are served by the same server.

Transparent failure bypassing to ensure 24x7 availability

Once any type of failure (server, operating system, WebLogic application server) is identified, Radware APSolute products automatically redirect users to operational resources.

Full disaster recovery and business continuity with Radware's global solution

Ensuring maximum availability of application resources in a single data center may not be enough in the face of natural or man-made disaster. In such cases all resources (servers, applications and WAN connections) are lost at the same time. In order to ensure BEA application availability even in such extreme conditions, application resources and infrastructure must be built across more than a single data center - in multiple locations.

Protection from Denial of Service (DoS) attacks

Denial of Service (DoS) attacks, such as Syn Floods and other application level floods, can paralyze critical applications and prevent legitimate users from accessing the application for the length of the attack. Radware APSolute security integrates several DoS protection mechanisms, which are based on attack tool pattern detection as well as traffic anomaly behavior analysis.

Protection from intrusions and application level attacks

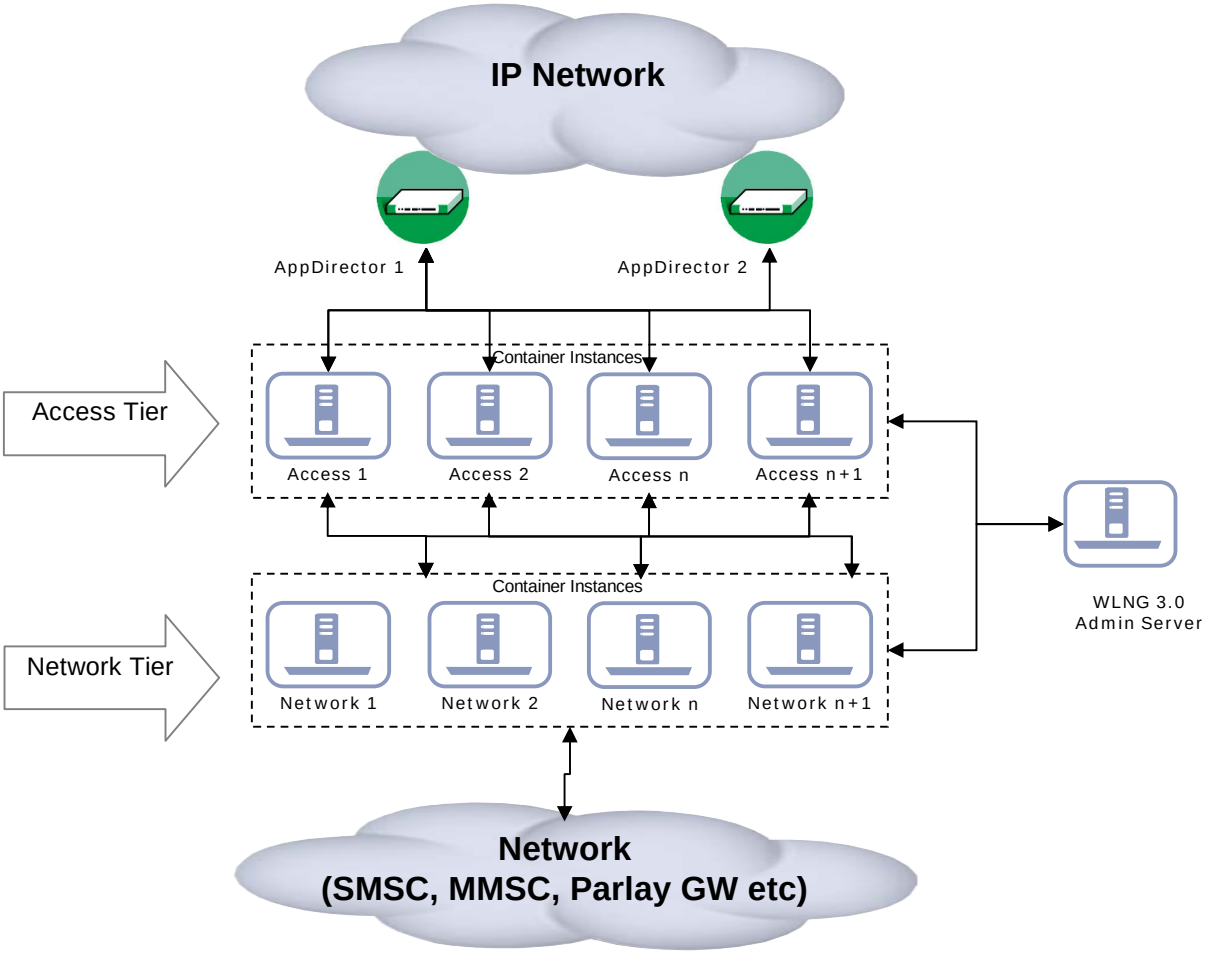
Intrusions and application level attacks may be targeted at the operating systems and the back end databases. The Radware APSolute Intrusion Prevention module identifies, in real time, through deep packet inspection, attack patterns and blocks them before getting to the application servers.

Solution Details

Weblogic Network Gatekeeper provides a two tier architecture

- Access Tier
  - Provides an entry point for 3rd party web services applications to connect to the Operators network
  - Authentication & Authorization of WS applications is done in this layer
  - Provides stateless access of service capabilities that are exposed by the network layer
- Network Tier
  - Provides access to the network resources
  - Network level service capabilities are exposed through this layer
  - Stateful protocol functions are maintained and managed by this layer

The AppDirector does monitor and load balance the access tier only.



How it works

Configuration

There are 2 different kind of TCP sessions between the WS client and the WLNG Access Tier server. The sendSmsRequest / sendSmsRespond session which is initiated on the client side. And the notifySMSDeliveryReceipt session that start on the server side.

1. The Appdirector is positioned inline and does work in the router mode.
2. The sendSmsRequest / sendSmsRespond session will be loadbalanced by the Appdirector with a L4-Policy.
3. The Server per Session Dispatch mode could be used for this application.
4. The sessions does have a short life-time so also the client aging time at the Appdirector could be reduced to 30 seconds in this test bed.
5. For the notifySMSDeliveryReceipt session it is important to enable the Server NAT option at the Appdirector
6. For the redundancy between the two AppDirector VRRP is used with a virtual Interfaces per subnet defined at the L4-Policy table.

Traffic Flow

TS SMS Messaging

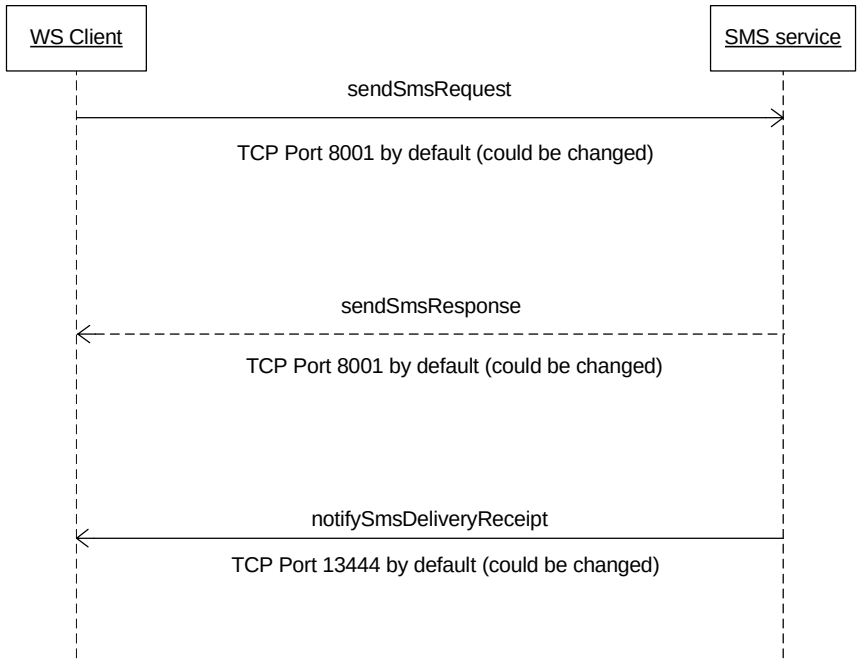
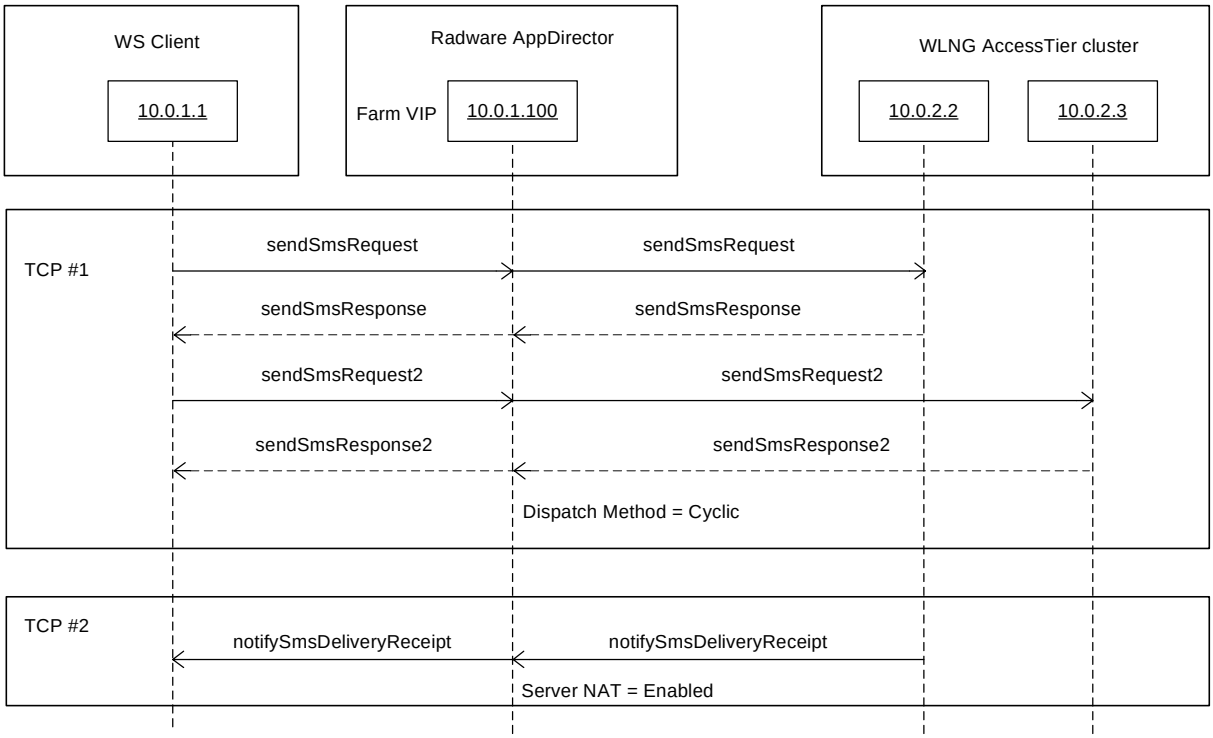


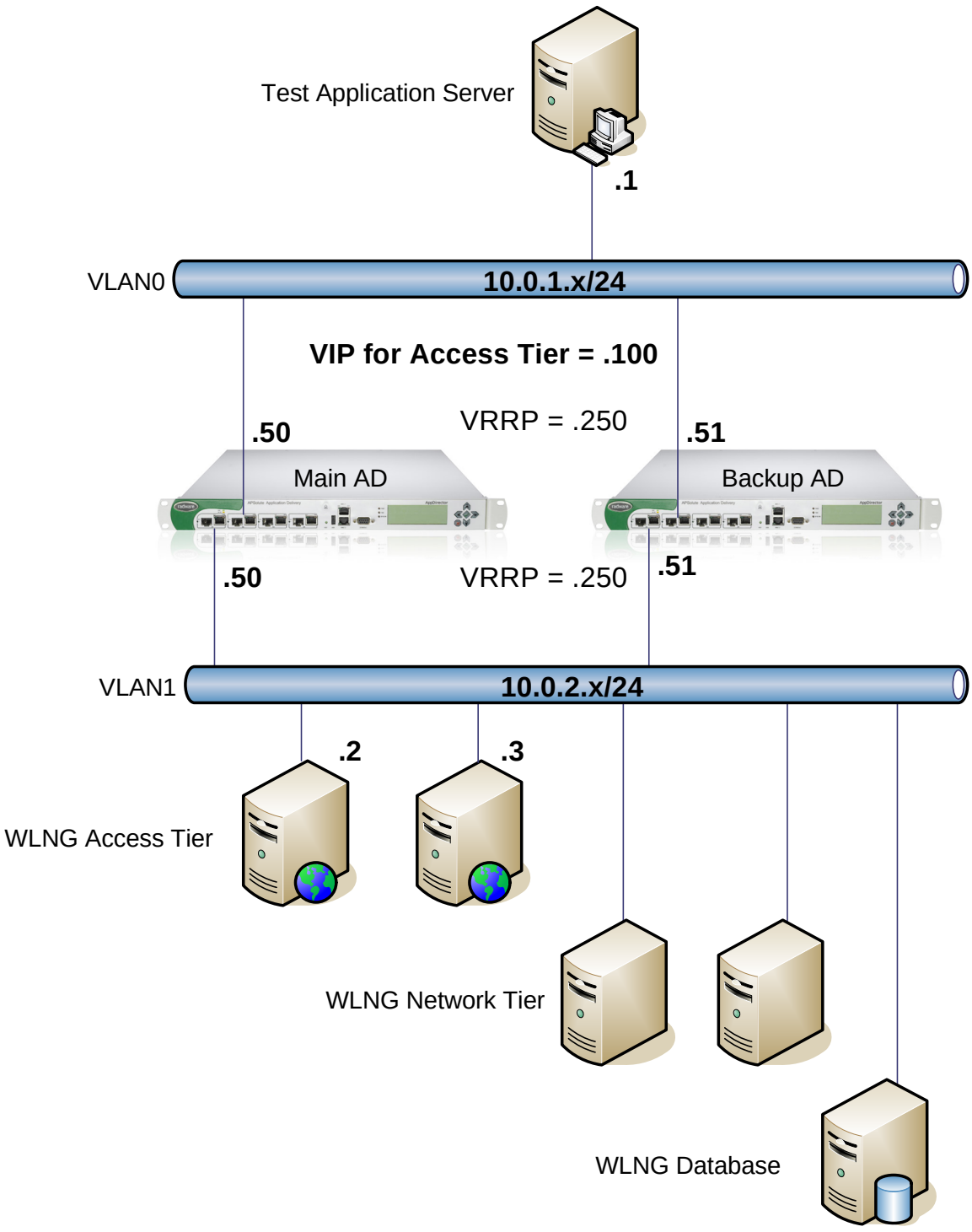
Figure 1 Send SMS sequence diagram



Software and Hardware used

Radware's AppDirector running Software Version 1.06.07 based on the ODS2 platform
BEA Systems WebLogic Network Gatekeeper 3.0 MP1.

Network Diagram



Configuration

The relevant part of this config is shown in BLUE for the:

- IP-Interface definition
- Default Gateway
- Farm, Server and L4-Policy creation
- Server NAT activation
- VRRP Redundancy

AppDirector (Main)

```
!
!Device Configuration
!Date: 11-04-2008 23:39:48
!DeviceDescription: AppDirector with Cookie Persistency
!Software Version: 1.06.07 (Build date Feb 21 2008, 23:40:16,Build#57)
!APSolute OS Version: 10.31-01.01(26):2.06.06

manage snmp versions-after-reset set "v1 & v2c & v3"

! IP-Interfaces and Default Gateway

net ip-interface create 10.10.100.169 255.255.255.0 17
net ip-interface create 10.0.2.50 255.255.255.0 2
net ip-interface create 10.0.1.50 255.255.255.0 1
net route table create 0.0.0.0 0.0.0.0 10.0.1.254 -i 1

! Farm, Server and L4-Policy creation

appdirector farm table setCreate WLNG_Farm -as Enabled -at 30 -dm \
"Fewest Number of Users" -cm "TCP Port" -cp 8001 -ci 3 -cr 2 -sm \
ServerPerSession
appdirector farm server table create WLNG_Farm 10.0.2.2 None -sn \
Access_Tier_1 -id 1
appdirector farm server table create WLNG_Farm 10.0.2.3 None -sn \
Access_Tier_2 -id 2
redundancy backup-in-vlan set disable
appdirector farm connectivity-check httpcode setCreate WLNG_Farm \
"200 - OK"
redundancy backup-fake-arp set enable
net next-hop-router setCreate 10.0.1.254 -fl 1
appdirector farm nhr setCreate 0.0.0.0 -ip 10.0.1.254 -fl 1
redundancy backup-interface-group set enable
appdirector segmentation nhr-table setCreate DefaultNHR -ip 10.0.1.254 \
-fl 1
appdirector l4-policy table create 10.0.1.100 TCP 8001 0.0.0.0 \
WLNG_TCP_8001 -fn WLNG_Farm
```

```
! Server NAT activation

appdirector nat server status set enable

! VRRP Redundancy

redundancy mode set VRRP
redundancy interface-group set enable
appdirector l4-policy table create 10.0.1.250 Any Any 0.0.0.0 VRRP_IP_G1 \
-ta "Virtual IP Interface"
appdirector l4-policy table create 10.0.2.250 Any Any 0.0.0.0 VRRP_IP_G2 \
-ta "Virtual IP Interface"
redundancy vrrp automated-config-update set Enabled
redundancy vrrp virtual-routers create 1 1 -as up -p 250 -pip 10.0.1.50
redundancy vrrp virtual-routers create 2 2 -as up -p 250 -pip 10.0.2.50
redundancy vrrp associated-ip create 1 1 10.0.1.250
redundancy vrrp associated-ip create 2 2 10.0.2.250
redundancy vrrp associated-ip create 1 1 10.0.1.100
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
redundancy arp-interface-group set Send
net l2-interface set 100001 -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 \
66630398707aaae049469015af589030 -pp DES -pkc \
66630398707aaae049469015af589030
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 \
UserBased -sn radware -sl authPriv
manage snmp community create public -n public -sn public
manage telnet session-timeout set 5
manage telnet auth-timeout set 30
redundancy force-down-ports-time set 0
appdirector global connectivity-check tcp-timeout set 3
```

AppDirector (Backup)

```
!
!Device Configuration
!Date: 11-04-2008 23:50:54
!DeviceDescription: AppDirector with Cookie Persistency
!Software Version: 1.06.07 (Build date Feb 21 2008, 23:40:16,Build#57)
!APSolute OS Version: 10.31-01.01(26):2.06.06

manage snmp versions-after-reset set "v1 & v2c & v3"

net ip-interface create 10.10.100.170 255.255.255.0 17
net ip-interface create 10.0.1.51 255.255.255.0 1
net ip-interface create 10.0.2.51 255.255.255.0 2
net route table create 0.0.0.0 0.0.0.0 10.0.1.254 -i 1
appdirector farm table setCreate WLNG_Farm -as Enabled -at 30 -dm \
"Fewest Number of Users" -cm "TCP Port" -cp 8001 -ci 3 -cr 2 -sm \
ServerPerSession
appdirector farm server table create WLNG_Farm 10.0.2.2 None -sn \
Access_Tier_1 -id 1
appdirector farm server table create WLNG_Farm 10.0.2.3 None -sn \
Access_Tier_2 -id 2
redundancy backup-in-vlan set disable
appdirector farm connectivity-check httpcode setCreate WLNG_Farm \
"200 - OK"
redundancy backup-fake-arp set enable
net next-hop-router setCreate 10.0.1.254 -fl 1
redundancy backup-interface-group set enable
appdirector l4-policy table create 10.0.1.100 TCP 8001 0.0.0.0 \
WLNG_TCP_8001 -fn WLNG_Farm -rs Backup
appdirector nat server status set enable
redundancy mode set VRRP
redundancy interface-group set disable
appdirector l4-policy table create 10.0.1.250 Any Any 0.0.0.0 VRRP_IP_G1 \
-ta "Virtual IP Interface"
appdirector l4-policy table create 10.0.2.250 Any Any 0.0.0.0 VRRP_IP_G2 \
-ta "Virtual IP Interface"
redundancy vrrp automated-config-update set Enabled
redundancy vrrp virtual-routers create 1 1 -pip 10.0.1.51
redundancy vrrp virtual-routers create 2 2 -pip 10.0.2.51
redundancy vrrp associated-ip create 1 1 10.0.1.250
redundancy vrrp associated-ip create 2 2 10.0.2.250
redundancy vrrp associated-ip create 1 1 10.0.1.100
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
redundancy arp-interface-group set Send
net l2-interface set 100001 -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 \
66630398707aaae049469015af589030 -pp DES -pkc \
66630398707aaae049469015af589030
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 \
UserBased -sn radware -sl authPriv
manage snmp community create public -n public -sn public
manage telnet session-timeout set 5
manage telnet auth-timeout set 30
redundancy force-down-ports-time set 0
appdirector global connectivity-check tcp-timeout set 3
```

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