

Implementing Radware Web Server Director In Oracle Application Server Enterprise Deployment

Oracle Corporation
Radware Ltd.

December 7, 2005

Oracle Corporation ©2005
Radware Ltd. ©2005

Contents

| | | |
|----------|---|-----------|
| 1 | Introduction | 1 |
| 2 | Network and Server Configuration | 1 |
| 2.1 | Server Configuration | 1 |
| 2.2 | Network Configuration | 1 |
| 2.3 | Routing Configuration | 2 |
| 2.3.1 | Routing Configuration on Firewall | 2 |
| 2.3.2 | Routing Configuraton on Servers | 5 |
| 3 | Radware WSD Configuration | 5 |
| 3.1 | Radware Equipment Required | 5 |
| 3.2 | Load Balancing Requirements | 5 |
| 3.3 | WSD Interface Configuration | 6 |
| 3.4 | Super-Farm Information on WSD | 6 |
| 3.5 | Farm Information on WSD | 6 |
| 3.6 | Server Information on WSD | 7 |
| 3.7 | Client NAT on WSD | 8 |
| 3.8 | Radware WSD Configuration | 8 |
| 4 | Radware CT100 Configuration | 11 |
| 4.1 | CT100 Interface Configuration | 11 |
| 4.2 | CT100 Tunnel Information | 11 |
| 4.3 | Radware CT100 Configuration | 11 |
| 4.3.1 | CT100-A Configuration | 11 |
| 4.3.2 | CT100-B Configuration | 16 |

1 Introduction

Web Server Director (WSD) by Radware is an intelligent application switch that delivers Layer 4-7 local and global switching across IP Applications such as web and database server farms, ensuring application uptime and global redundancy as well as user experience optimization. CertainT 100 (CT100) accelerates application performance through Web compression, HTTP multiplexing and SSL offloading from servers for the fastest application response times and scalable SSL handling. Used together, WSD and CT100 provide availability, high performance and complete security for mission critical applications.

Radware WSD can be used as application load balance router (LBR) in Oracle Application Server 10g Release 2 (10.1.2) enterprise deployment architecture.

This document describes a sample configuration of Radware WSD (with software version 8.16.13) and CT100 (with software version 3.21.07) implemented in an Oracle Application Server 10g Release 2 (10.1.2) enterprise deployment architecture. This architecture is implemented in an imaginary Internet domain called *pdx.com*. The sample domain name *pdx.com* should be replaced by appropriate Internet domain in reality. The sample configuration of Radware WSD was fully tested and certified for use with Oracle Application Server 10g Release 2 (10.1.2).

2 Network and Server Configuration

2.1 Server Configuration

There are 10 servers required in this enterprise deployment architecture for OracleAS portal application. The following is the list of these 10 servers:

| Server Name | IP Address | Subnet Mask | Function |
|--------------|---------------|---------------|--------------------------------|
| Apphost1 | 192.168.0.205 | 255.255.255.0 | WebCache and Web Server 1 |
| Apphost2 | 192.168.0.206 | 255.255.255.0 | WebCache and Web Server 2 |
| Idmhost1 | 192.168.0.199 | 255.255.255.0 | Identity Management Server 1 |
| Idmhost2 | 192.168.0.201 | 255.255.255.0 | Identity Management Server 2 |
| Oidhost1 | 192.168.2.200 | 255.255.255.0 | OID Server 1 |
| Oidhost2 | 192.168.2.201 | 255.255.255.0 | OID Server 2 |
| Infradbhost1 | 192.168.2.202 | 255.255.255.0 | DB Server for Infrastructure 1 |
| Infradbhost2 | 192.168.2.203 | 255.255.255.0 | DB Server for Infrastructure 2 |
| Appdbhost1 | 192.168.2.204 | 255.255.255.0 | DB Server for Application 1 |
| Appdbhost2 | 192.168.2.205 | 255.255.255.0 | DB Server for Application 2 |

2.2 Network Configuration

Three subnets are used in the configuration, including:

| Zone | Network | Netmask |
|----------|---------------|---------------|
| External | 192.168.200.0 | 255.255.255.0 |
| DMZ1 | 192.168.0.0 | 255.255.255.0 |
| DMZ2 | 192.168.2.0 | 255.255.255.0 |

There are three SuperFarm Virtual IP addresses (VIPs) configured on WSD:

| VIP | IP | Host | Ports |
|------|----------------|-----------------|------------------------|
| VIP1 | 192.168.200.11 | portal.pdx.com | 80, 443, 7777 and 9401 |
| VIP2 | 192.168.200.10 | login.pdx.com | 80, 443 and 7777 |
| VIP3 | 192.168.0.155 | oidhost.pdx.com | 389 and 636 |

The Figure 1 on page 3 and the Figure 2 on page 4 demonstrate all major network components involved in this sample configuration of the Radware WSD (with software version 8.16.13) and CT100 (with software version 3.21.07) implemented in an Oracle Application Server 10g Release 2 (10.1.2) enterprise deployment architecture. The Figure 1 is more towards a logical view of network configuration, while the Figure 2 is more towards a physical view of the network configuration. Note that two logical load balance routers (LBRs) in the Figure 1 is implemented as a physical load balance router with Radware WSD in the Figure 2.

2.3 Routing Configuration

Routing configuration can be done in two different ways: either on servers or on firewall. Both from security and management point of view, configuring routing on firewall is a preferable way to handle routing issue in this deployment. But improper routing configuration on firewall may cause strange routing issues. On the other hand, the advantage of configuring routing on servers is probably some small performance gain because the connections to VIPs do not have to go through the extra hop on the firewall. Both approaches were tested working in our testing environment. Routing implementation depends on the overall requirements of the application.

2.3.1 Routing Configuration on Firewall

In this approach, the default gateway for each server should be the appropriate interface on the firewall. The IP address for the interface on the firewall should be on the same subnet as the server. In our deployment, the default gateway for all servers on 192.168.0.0/24 subnet is 192.168.0.200 on firewall while the default gateway for all servers on 192.168.2.0/24 subnet is 192.168.2.1 on firewall, referring the Figure 2.

In addition, on the firewall, add a static route for each VIP so that the next hop gateway to each VIP is the IP address of an interface on Radware WSD. This interface should be on the VIP's corresponding servers' subnet. The following routing configured on the firewall was tested working in our deployment:

| Destination | Gateway | Netmask |
|----------------|-------------|-----------------|
| 192.168.200.10 | 192.168.0.1 | 255.255.255.255 |
| 192.168.200.11 | 192.168.0.1 | 255.255.255.255 |
| 192.168.0.155 | 192.168.2.2 | 255.255.255.255 |
| 192.168.2.0 | 0.0.0.0 | 255.255.255.0 |
| 192.168.0.0 | 0.0.0.0 | 255.255.255.0 |
| 0.0.0.0 | 192.168.0.1 | 0.0.0.0 |

Note that the servers mapped by the VIP1 192.168.200.10 and servers mapped by the VIP2 192.168.200.11 are on the 192.168.0.x subnet and that the servers mapped by the VIP3 192.168.0.155 are on the 192.168.2.x subnet.

In order to enhance security, firewall policy can be implemented to control which ports should be open and which ports should be closed for any given pairs of source and destination addresses.

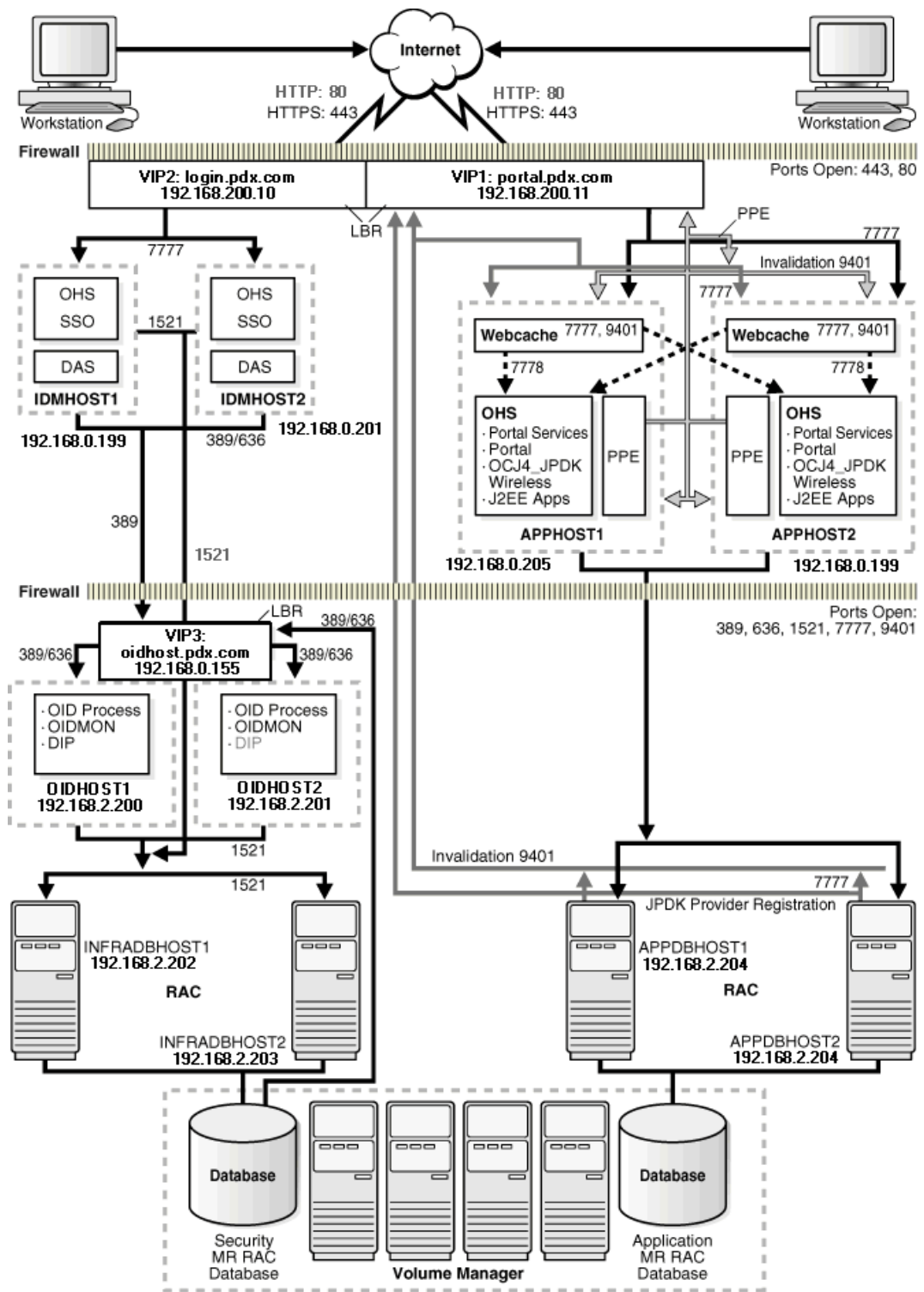


Figure 1: Network Configuration - Logical View

2.3.2 Routing Configuraton on Servers

In general, in this approach, static routes on every server should be configured to ensure that the server can access VIPs through and only through appropriate interfaces on Radware WSD.

For example, since Appdbhost1 and Appdbhost2 are required to have access to VIP1 for invalidation on port 9401 as shown in the Figure 1, a static route on both Appdbhost1 and Appdbhost2 should be configured so that the destination address VIP1 (192.168.200.11) can be accessed through and only through 192.168.2.2 on WSD, although the default gateway can be 192.168.2.1 on the firewall for Appdbhost1 and Appdbhost2, as shown in the Figure 2.

The following is a sample routing table on Appdbhost1 and Appdbhost2:

| Destination | Gateway | Netmask |
|----------------|-------------|-----------------|
| 192.168.200.10 | 192.168.2.2 | 255.255.255.255 |
| 192.168.200.11 | 192.168.2.2 | 255.255.255.255 |
| 192.168.0.155 | 192.168.2.2 | 255.255.255.255 |
| 192.168.2.0 | 0.0.0.0 | 255.255.255.0 |
| 0.0.0.0 | 192.168.2.1 | 0.0.0.0 |

3 Radware WSD Configuration

In this sample configuration, one Radware WSD (software version 8.16.13) is used as the main load balancer (LBR). In addition, two Radware CertainT 100 (CT100) SSL Accelerators (software version 3.21.07) are deployed to serve https requests in a farm configuration, effectively offloading intensive SSL calculations from web server CPU's. Combining Radware CertainT 100 with Radware WSD results in the high quality user experience.

3.1 Radware Equipment Required

1. One Radware WSD (software version 8.16.13) named WSD;

Note:

- If additional resiliency is desired, a redundant WSD can be deployed in a high availability configuration.
2. Two Radware CertainT 100 (software version 3.21.07) SSL Accelerators named CT100-A and CT100-B.

3.2 Load Balancing Requirements

The following is the list of VIP requirements for Radware WSD for load balancing purpose:

| Load Balancing Requirements | | | |
|-----------------------------|---|--------------------|--------------------|
| 192.168.200.11:80 | → | 192.168.0.205:7777 | |
| | | 192.168.0.206:7777 | |
| 192.168.200.11:7777 | → | 192.168.0.205:7777 | |
| | | 192.168.0.206:7777 | |
| 192.168.200.11:9401 | → | 192.168.0.205:9401 | |
| | | 192.168.0.206:9401 | |
| 192.168.200.11:443 | → | SSL Accelerators → | 192.168.0.205:7777 |
| | | | 192.168.0.206:7777 |
| 192.168.200.10:80 | → | 192.168.0.199:7777 | |
| | | 192.168.0.201:7777 | |
| 192.168.200.10:7777 | → | 192.168.0.199:7777 | |
| | | 192.168.0.201:7777 | |
| 192.168.200.10:443 | → | SSL Accelerators → | 192.168.0.199:7777 |
| | | | 192.168.0.201:7777 |
| 192.168.0.155:389 | → | 192.168.2.200:389 | |
| | | 192.168.2.201:389 | |
| 192.168.0.155:636 | → | 192.168.2.200:636 | |
| | | 192.168.2.201:636 | |

3.3 WSD Interface Configuration

The Radware WSD interfaces required in the deployment are configured as following:

| Interface | IP Address | Subnet Mask |
|-----------|---------------|---------------|
| 1 | 192.168.0.1 | 255.255.255.0 |
| 3 | 192.168.2.2 | 255.255.255.0 |
| 4 | 192.168.200.5 | 255.255.255.0 |
| 5 | 10.1.0.1 | 255.255.255.0 |

3.4 Super-Farm Information on WSD

The following is the information about super-farms required for the deployment:

| Super-Farm | Port | Protocol | Farm |
|----------------|------|----------|----------|
| 192.168.0.155 | 389 | TCP | 10.0.3.1 |
| | 636 | TCP | 10.0.3.2 |
| 192.168.200.10 | 80 | TCP | 10.0.2.1 |
| | 7777 | TCP | 10.0.2.2 |
| | 443 | TCP | 10.0.2.4 |
| 192.168.200.11 | 80 | TCP | 10.0.1.1 |
| | 7777 | TCP | 10.0.1.2 |
| | 9401 | TCP | 10.0.1.3 |
| | 443 | TCP | 10.0.1.5 |

3.5 Farm Information on WSD

The following is the information about farms required for the deployment:

| IP Address | Dispatch Method ¹ | Multiplexed Farm Port ² |
|------------|------------------------------|------------------------------------|
| 10.0.1.1 | Cyclic | 80 |
| 10.0.1.2 | Cyclic | No Multiplexing |
| 10.0.1.3 | Cyclic | No Multiplexing |
| 10.0.1.4 | Cyclic | No Multiplexing |
| 10.0.1.5 | Cyclic | No Multiplexing |
| 10.0.2.1 | Cyclic | 80 |
| 10.0.2.2 | Cyclic | No Multiplexing |
| 10.0.2.3 | Cyclic | No Multiplexing |
| 10.0.2.4 | Cyclic | No Multiplexing |
| 10.0.3.1 | Cyclic | No Multiplexing |
| 10.0.3.2 | Cyclic | No Multiplexing |

Note:

1. Although not tested in this sample configuration, several additional Dispatch Methods are available on Radware's WSD, including Weighted Cyclic, Least Amount of Traffic, Fewest Number of Users, and based on Response Time.
2. A Multiplexed Farm Port enables applications on the servers to be available on ports other than the port intercepted by the Farm.

3.6 Server Information on WSD

The following is the information about application servers required for the deployment:

| Farm | Server | Server Name | Multiplexed Server Port |
|----------|---------------|-------------|-------------------------|
| 10.0.1.1 | 192.168.0.205 | apphost1 | 7777 |
| | 192.168.0.206 | apphost2 | 7777 |
| 10.0.1.2 | 192.168.0.205 | apphost1 | No Multiplexing |
| | 192.168.0.206 | apphost2 | No Multiplexing |
| 10.0.1.3 | 192.168.0.205 | apphost1 | No Multiplexing |
| | 192.168.0.206 | apphost2 | No Multiplexing |
| 10.0.1.4 | 192.168.0.205 | apphost1 | No Multiplexing |
| | 192.168.0.206 | apphost2 | No Multiplexing |
| 10.0.1.5 | 10.1.0.11 | ct100_a_t1 | No Multiplexing |
| | 10.1.0.21 | ct100_b_t1 | No Multiplexing |
| 10.0.2.1 | 192.168.0.199 | idmhost1 | 7777 |
| | 192.168.0.201 | idmhost2 | 7777 |
| 10.0.2.2 | 192.168.0.199 | idmhost1 | No Multiplexing |
| | 192.168.0.201 | idmhost2 | No Multiplexing |
| 10.0.2.3 | 192.168.0.199 | idmhost1 | No Multiplexing |
| | 192.168.0.201 | idmhost2 | No Multiplexing |
| 10.0.2.4 | 10.1.0.12 | ct100_a_t2 | No Multiplexing |
| | 10.1.0.22 | ct100_b_t2 | No Multiplexing |
| 10.0.3.1 | 192.168.2.200 | oidhost1 | No Multiplexing |
| | 192.168.2.201 | oidhost2 | No Multiplexing |
| 10.0.3.2 | 192.168.2.200 | oidhost1 | No Multiplexing |
| | 192.168.2.201 | oidhost2 | No Multiplexing |

3.7 Client NAT on WSD

In order for Oracle Application Server to work with Radware WSD properly, Client NAT should be enabled on Radware WSD. Ideally, every VIP should use a unique range of Client NAT addresses. In order to avoid unnecessary routing issues, an client NAT address corresponding to a VIP should be on the same subnet as the servers the VIP points to. In addition, appropriate routing should be configured either on firewall or on servers, as discussed in section 2.3.

3.8 Radware WSD Configuration

The following is an excerpt of the WSD configuration. Only the configuration commands applicable to the sample configuration are shown.

Note:

- The “\” character indicates that a command is continued on the next line;
- Command order and comment characters (“!”) are added for readability.

```
!Base MAC Address: 00:03:b2:1f:53:40
!Date: 01-12-2005 01:57:18
!Device Configuration
!DeviceDescription: Web Server Director DS with SynApps (512 farms)
!Software Version: 8.16.13 (build 5fe9c8)
!
!The following command requires resetting the device to take effect.
!
system tune nat-address-table set 10
!
system mib2-name set WSD-1
!
net ip-interface create 192.168.0.1 255.255.255.0 1
net ip-interface create 192.168.2.2 255.255.255.0 3
net ip-interface create 192.168.200.5 255.255.255.0 4
net ip-interface create 10.1.0.1 255.255.255.0 5
net route table create 0.0.0.0 0.0.0.0 192.168.200.1 -i 4
net physical-interface set 1 -s "Fast Ethernet" -d Full
net physical-interface set 3 -s "Fast Ethernet" -d Full
net physical-interface set 4 -s "Fast Ethernet" -d Full
net physical-interface set 5 -s "Fast Ethernet" -d Full
!
wsd farm table create 10.0.1.1 -n portal.pdx.com:80 -as Enabled -dm Cyclic \
-cm "TCP Port" -cp 7777 -mp 80 -sm EntryPerSession
wsd farm table create 10.0.1.2 -n portal.pdx.com:7777 -as Enabled -dm \
Cyclic -cm "TCP Port" -cp 7777 -sm EntryPerSession
wsd farm table create 10.0.1.3 -n portal.pdx.com:9401 -as Enabled -dm \
Cyclic -cm "TCP Port" -cp 9401 -sm EntryPerSession
wsd farm table create 10.0.1.4 -n "portal.pdx.com:443 Server Farm " -as \
Enabled -dm Cyclic -cm "TCP Port" -cp 7777 -sm EntryPerSession
wsd farm table create 10.0.1.5 -n "portal.pdx.com:443 CT100 Farm " -as \
Enabled -dm Cyclic -cm "TCP Port" -cp HTTPS -sm EntryPerSession
wsd farm table create 10.0.2.1 -n login.pdx.com:80 -as Enabled -dm Cyclic \
```

```

-cm "TCP Port" -cp 7777 -mp 80 -sm EntryPerSession
wsd farm table create 10.0.2.2 -n login.pdx.com:7777 -as Enabled -dm Cyclic \
-cm "TCP Port" -cp 7777 -sm EntryPerSession
wsd farm table create 10.0.2.3 -n "login.pdx.com:443 Server Farm" -as \
Enabled -dm Cyclic -cm "TCP Port" -cp 7777 -sm EntryPerSession
wsd farm table create 10.0.2.4 -n "login.pdx.com:443 CT100 Farm" -as \
Enabled -dm Cyclic -cm "TCP Port" -cp HTTPS -sm EntryPerSession
wsd farm table create 10.0.3.1 -n oidhost.pdx.com:389 -as Enabled -dm \
Cyclic -cm "TCP Port" -cp 389 -sm EntryPerSession
wsd farm table create 10.0.3.2 -n oidhost.pdx.com:636 -as Enabled -dm \
Cyclic -cm "TCP Port" -cp 636 -sm EntryPerSession
!
wsd farm extended-params set 10.0.1.1 -nr 192.168.0.241
wsd farm extended-params set 10.0.1.2 -nr 192.168.0.242
wsd farm extended-params set 10.0.1.3 -nr 192.168.0.243
wsd farm extended-params set 10.0.1.4 -nr 192.168.0.244 -as Enabled
wsd farm extended-params set 10.0.1.5 -as Enabled
wsd farm extended-params set 10.0.2.1 -nr 192.168.0.245
wsd farm extended-params set 10.0.2.2 -nr 192.168.0.246
wsd farm extended-params set 10.0.2.3 -nr 192.168.0.247 -as Enabled
wsd farm extended-params set 10.0.2.4 -as Enabled
wsd farm extended-params set 10.0.3.1 -nr 192.168.2.241
wsd farm extended-params set 10.0.3.2 -nr 192.168.2.242
!
wsd farm server table create 10.0.1.1 192.168.0.205 -sn apphost1 -mp 7777 \
-cn Enabled -sd apphost1
wsd farm server table create 10.0.1.1 192.168.0.206 -sn apphost2 -mp 7777 \
-cn Enabled -sd apphost2
wsd farm server table create 10.0.1.2 192.168.0.205 -sn apphost1 -cn \
Enabled -sd apphost1
wsd farm server table create 10.0.1.2 192.168.0.206 -sn apphost2 -cn \
Enabled -sd apphost2
wsd farm server table create 10.0.1.3 192.168.0.205 -sn apphost1 -cn \
Enabled -sd apphost1
wsd farm server table create 10.0.1.3 192.168.0.206 -sn apphost2 -cn \
Enabled -sd apphost2
wsd farm server table create 10.0.1.4 192.168.0.205 -sn apphost1 -cn \
Enabled -sd apphost1
wsd farm server table create 10.0.1.4 192.168.0.206 -sn apphost2 -cn \
Enabled -sd apphost2
wsd farm server table create 10.0.1.5 10.1.0.11 -sn ct100_a_t1 -sd \
CT100 Unit A Tunnel 1
wsd farm server table create 10.0.1.5 10.1.0.21 -sn ct100_b_t1 -sd \
CT100 Unit B Tunnel 1
wsd farm server table create 10.0.2.1 192.168.0.199 -sn idmhost1 -mp 7777 \
-cn Enabled -sd idmhost1
wsd farm server table create 10.0.2.1 192.168.0.201 -sn idmhost2 -mp 7777 \
-cn Enabled -sd idmhost2
wsd farm server table create 10.0.2.2 192.168.0.199 -sn idmhost1 -cn \

```

```

Enabled -sd idmhost1
wsd farm server table create 10.0.2.2 192.168.0.201 -sn idmhost2 -cn \
Enabled -sd idmhost2
wsd farm server table create 10.0.2.3 192.168.0.199 -sn idmhost1 -cn \
Enabled -sd idmhost1
wsd farm server table create 10.0.2.3 192.168.0.201 -sn idmhost2 -cn \
Enabled -sd idmhost2
wsd farm server table create 10.0.2.4 10.1.0.12 -sn ct100_a_t2 -sd \
CT100 Unit A Tunnel 2
wsd farm server table create 10.0.2.4 10.1.0.22 -sn ct100_b_t2 -sd \
CT100 Unit B Tunnel 2
wsd farm server table create 10.0.3.1 192.168.2.200 -sn oidhost1 -cn \
Enabled -sd oidhost1
wsd farm server table create 10.0.3.1 192.168.2.201 -sn oidhost2 -cn \
Enabled -sd oidhost2
wsd farm server table create 10.0.3.2 192.168.2.200 -sn oidhost1 -cn \
Enabled -sd oidhost1
wsd farm server table create 10.0.3.2 192.168.2.201 -sn oidhost2 -cn \
Enabled -sd oidhost2
!
wsd global client-table open-new-entry set enable
wsd global client-table select-server set enable
!
wsd nat client address-range create 192.168.0.241 -t 192.168.0.241
wsd nat client address-range create 192.168.0.242 -t 192.168.0.242
wsd nat client address-range create 192.168.0.243 -t 192.168.0.243
wsd nat client address-range create 192.168.0.244 -t 192.168.0.244
wsd nat client address-range create 192.168.0.245 -t 192.168.0.245
wsd nat client address-range create 192.168.0.246 -t 192.168.0.246
wsd nat client address-range create 192.168.0.247 -t 192.168.0.247
wsd nat client address-range create 192.168.2.241 -t 192.168.2.241
wsd nat client address-range create 192.168.2.242 -t 192.168.2.242
wsd nat client range-to-nat create 0.0.0.0 -t 255.255.255.255
wsd nat client status set enable
!
wsd super-farm create 192.168.0.155 389 TCP 10.0.3.1
wsd super-farm create 192.168.0.155 636 TCP 10.0.3.2
wsd super-farm create 192.168.200.10 443 TCP 10.0.2.4
wsd super-farm create 192.168.200.10 7777 TCP 10.0.2.2
wsd super-farm create 192.168.200.10 80 TCP 10.0.2.1
wsd super-farm create 192.168.200.11 443 TCP 10.0.1.5
wsd super-farm create 192.168.200.11 7777 TCP 10.0.1.2
wsd super-farm create 192.168.200.11 80 TCP 10.0.1.1
wsd super-farm create 192.168.200.11 9401 TCP 10.0.1.3
!
health-monitoring status set enable
health-monitoring check create apphost1:7777 -m HTTP -d 192.168.0.205 -p \
7777 -rt Enabled
health-monitoring check create apphost1:9401 -m "TCP Port" -d 192.168.0.205 \

```

```

-p 9401 -rt Enabled
health-monitoring check create apphost2:7777 -m HTTP -d 192.168.0.206 -p \
7777 -rt Enabled
health-monitoring check create apphost2:9401 -m "TCP Port" -d 192.168.0.206 \
-p 9401 -rt Enabled
health-monitoring check create idmhost1:7777 -m HTTP -d 192.168.0.199 -p \
7777 -rt Enabled
health-monitoring check create idmhost2:7777 -m HTTP -d 192.168.0.201 -p \
7777 -rt Enabled
health-monitoring check create oidhost1:389 -m "TCP Port" -d 192.168.2.200 \
-p 389 -rt Enabled
health-monitoring check create oidhost1:636 -m "TCP Port" -d 192.168.2.200 \
-p 636 -rt Enabled
health-monitoring check create oidhost2:389 -m "TCP Port" -d 192.168.2.201 \
-p 389 -rt Enabled
health-monitoring check create oidhost2:636 -m "TCP Port" -d 192.168.2.201 \
-p 636 -rt Enabled

```

4 Radware CT100 Configuration

4.1 CT100 Interface Configuration

The following is the interface configuration for CT100 units:

| CT100 Unit | Interface | IP Address | Netmask |
|------------|-----------|------------|---------------|
| CT100-A | 1 | 10.1.0.10 | 255.255.255.0 |
| CT100-B | 1 | 10.1.0.20 | 255.255.255.0 |

4.2 CT100 Tunnel Information

The following is the tunnel configuration for CT100 units:

| CT100 Unit | Virtual Host IP | Listen Port | Remote IP | Remote Port |
|------------|-----------------|-------------|-----------|-------------|
| CT100-A | 10.1.0.12 | 443 | 10.0.2.3 | 7777 |
| CT100-A | 10.1.0.11 | 443 | 10.0.1.4 | 7777 |
| CT100-B | 10.1.0.22 | 443 | 10.0.2.3 | 7777 |
| CT100-B | 10.1.0.21 | 443 | 10.0.1.4 | 7777 |

4.3 Radware CT100 Configuration

4.3.1 CT100-A Configuration

The following is an excerpt of CT100-A's configuration. Only the parameters applicable to the sample configuration are shown.

```

-----
                CertainT 100 Configuration
-----

```

```

ct key get

```

Keys:

| Index | Size | Cert | Common Name |
|-------|------|------|----------------|
| 3 | 1024 | Crt | portal.pdx.com |
| 4 | 1024 | Crt | login.pdx.com |

ct key get <Key ID>

Info for Key number 3 :

Certificate (csr/crt/int) = crt
Date not before = Nov 22 11:53:14 2005 GMT
Date not after = Nov 22 11:53:14 2006 GMT
Key Size (512/1024/2048) = 1024
Common Name = portal.pdx.com

This Key is not attached to a Proxy.

Tunnel IP / Server Name

3 .

Info for Key number 4 :

Certificate (csr/crt/int) = crt
Date not before = Nov 22 11:59:20 2005 GMT
Date not after = Nov 22 11:59:20 2006 GMT
Key Size (512/1024/2048) = 1024
Common Name = login.pdx.com

This Key is not attached to a Proxy.

Tunnel IP / Server Name

2 .

ct mode get

Active mode is: proxy

ct tunnel get

Tunnels:

| Index | Enabled | Virtual Host IP | Listen Port | Remote IP | Remote Port | Key ID |
|-------|---------|-----------------|-------------|-----------|-------------|--------|
| 2 | yes | 10.1.0.12 | 443 | 10.0.2.3 | 7777 | 4 |
| 3 | yes | 10.1.0.11 | 443 | 10.0.1.4 | 7777 | 3 |

ct tunnel get <Key ID>

Tunnel info for Tunnel ID 2 :

```
Enabled : yes
LAN : 1
Virtual Host IP : 10.1.0.12
Listening Port : 443
Interface IP : 10.1.0.12
Netmask : 255.255.255.0
Remote IP : 10.0.2.3
Remote Port : 7777
Transparent : on
Hostname : .
Keep Alive : on
Keep Alive Timeout : 15
Compression method : gzip
Gzip engine : hw
Gzip threshold : 1024
HTTP redirect : off
HTTP redirect port : 0
HTTPS redirect : off
HTTP multiplexing : off
HTTP multiplexing timeout : 0
HTTP garbage : off
SSL Key ID : 4
CipherSuites : RSA
Backend SSL : off
Backend CipherSuites : LOW
Backend L7 LB port : 0
Service : http
Client CA : no
CRL : no
Client Timeout : 30
Backend Timeout : 300
Cdp tunnel bindings : none
```

```

Tunnel info for Tunnel ID      3 :
=====
Enabled                          : yes
LAN                              : 1
Virtual Host IP                  : 10.1.0.11
Listening Port                   : 443
Interface IP                     : 10.1.0.11
Netmask                          : 255.255.255.0
Remote IP                        : 10.0.1.4
Remote Port                      : 7777
Transparent                      : on
Hostname                         : .
Keep Alive                      : on
Keep Alive Timeout               : 15
Compression method               : gzip
Gzip engine                      : hw
Gzip threshold                   : 1024
HTTP redirect                   : off
HTTP redirect port               : 0
HTTPS redirect                   : off
HTTP multiplexing                : off
HTTP multiplexing timeout       : 0
HTTP garbage                     : off
SSL Key ID                      : 3
CipherSuites                    : RSA
Backend SSL                      : off
Backend CipherSuites            : LOW
Backend L7 LB port               : 0
Service                         : http
Client CA                       : no
CRL                             : no
Client Timeout                   : 30
Backend Timeout                  : 300
Cdp tunnel bindings              : none

```

```

-----
Network Configuration
-----

```

```

net management-ip get
-----

```

```

Management interfaces:

```

```

|-----|-----|-----|
| IP Address | Net Mask | Interface |
|=====|=====|=====|
| 10.1.0.10 | 255.255.255.0 | Lan1 |
|-----|-----|-----|

```

```
net physical-interface get
```

```
-----
```

```
Current mode:
```

```
LAN 1 : Speed of 100 Mbps and a duplex mode of full
```

```
LAN 2 : Autodetection mode
```

```
net route get
```

```
-----
```

```
Configured Routing Table:
```

| Type | Destination | Netmask | Gateway |
|---------|-------------|---------|----------|
| Default | | | 10.1.0.1 |

```
Active Interface Routing Table:
```

| Type | Destination | Netmask | Gateway |
|---------|-------------|---------|----------|
| Default | | | 10.1.0.1 |

```
-----  
System Configuration  
-----
```

```
system device info get
```

```
-----
```

```
Device model: D.
```

```
Software version: 3.21.07 Build Oct_03_2005_09-09-12.
```

```
License level: 3.
```

```
TPS: 2800.
```

```
Concurrent connections: 6000.
```

```
RAM size: 512 MB.
```

```
Mac Lan 1: 000423B5A9FA.
```

```
Mac Lan 2: 0010F30677CF.
```

```
system device name get
```

```
-----
```

```
The current device name is CT100A.
```

```
system mode get
```

```
-----
```

Current system mode is: active

4.3.2 CT100-B Configuration

The following is an excerpt of CT100-B's configuration. Only the parameters applicable to the sample configuration are shown.

```
-----  
                CertainT 100 Configuration  
-----  
  
ct key get  
-----  
  
Keys:  
  
|-----|-----|-----|-----|  
| Index | Size | Cert | Common Name |  
|=====|=====|=====|=====|  
|   1   | 1024 | Crt  | www.radware.com |  
|   2   | 1024 | Crt  | www.radware.com |  
|   3   | 1024 | Crt  | portal.pdx.com  |  
|   4   | 1024 | Crt  | login.pdx.com   |  
|-----|-----|-----|-----|
```

```
ct key get <Key ID>  
-----
```

```
Info for Key number 3 :  
-----  
Certificate (csr/crt/int) = crt  
Date not before           = Nov 22 11:53:14 2005 GMT  
Date not after            = Nov 22 11:53:14 2006 GMT  
Key Size (512/1024/2048) = 1024  
Common Name                = portal.pdx.com
```

This Key is not attached to a Proxy.

```
Tunnel IP / Server Name  
-----  
3 .
```

```
Info for Key number 4 :  
-----  
Certificate (csr/crt/int) = crt
```

Date not before = Nov 22 11:59:20 2005 GMT
Date not after = Nov 22 11:59:20 2006 GMT
Key Size (512/1024/2048) = 1024
Common Name = login.pdx.com

This Key is not attached to a Proxy.

Tunnel IP / Server Name

2 .

ct tunnel get

Tunnels:

| Index | Enabled | Virtual Host IP | Listen Port | Remote IP | Remote Port | Key ID |
|-------|---------|-----------------|-------------|-----------|-------------|--------|
| 2 | yes | 10.1.0.22 | 443 | 10.0.2.3 | 7777 | 4 |
| 3 | yes | 10.1.0.21 | 443 | 10.0.1.4 | 7777 | 3 |

ct tunnel get <Key ID>

Tunnel info for Tunnel ID 2 :

=====

Enabled : yes
LAN : 1
Virtual Host IP : 10.1.0.22
Listening Port : 443
Interface IP : 10.1.0.22
Netmask : 255.255.255.0
Remote IP : 10.0.2.3
Remote Port : 7777
Transparent : on
Hostname : .
Keep Alive : on
Keep Alive Timeout : 15
Compression method : gzip
Gzip engine : hw
Gzip threshold : 1024
HTTP redirect : off
HTTP redirect port : 0

HTTPS redirect : off
HTTP multiplexing : off
HTTP multiplexing timeout : 0
HTTP garbage : off
SSL Key ID : 4
CipherSuites : RSA
Backend SSL : off
Backend CipherSuites : LOW
Backend L7 LB port : 0
Service : http
Client CA : no
CRL : no
Client Timeout : 30
Backend Timeout : 300
Cdp tunnel bindings : none

Tunnel info for Tunnel ID 3 :

=====

Enabled : yes
LAN : 1
Virtual Host IP : 10.1.0.21
Listening Port : 443
Interface IP : 10.1.0.21
Netmask : 255.255.255.0
Remote IP : 10.0.1.4
Remote Port : 7777
Transparent : on
Hostname : .
Keep Alive : on
Keep Alive Timeout : 15
Compression method : gzip
Gzip engine : hw
Gzip threshold : 1024
HTTP redirect : off
HTTP redirect port : 0
HTTPS redirect : off
HTTP multiplexing : off
HTTP multiplexing timeout : 0
HTTP garbage : off
SSL Key ID : 3
CipherSuites : RSA
Backend SSL : off
Backend CipherSuites : LOW
Backend L7 LB port : 0
Service : http
Client CA : no
CRL : no

```
Client Timeout      : 30
Backend Timeout    : 300
Cdp tunnel bindings : none
```

```
-----
                        Network Configuration
-----
```

```
net management-ip get
-----
```

Management interfaces:

| IP Address | Net Mask | Interface |
|------------|---------------|-----------|
| 10.1.0.20 | 255.255.255.0 | Lan1 |

```
net physical-interface get
-----
```

Current mode:

```
LAN 1 : Speed of 100 Mbps and a duplex mode of full
LAN 2 : Autodetection mode
```

```
net route get
-----
```

Configured Routing Table:

| Type | Destination | Netmask | Gateway |
|---------|-------------|---------|----------|
| Default | | | 10.1.0.1 |

Active Interface Routing Table:

| Type | Destination | Netmask | Gateway |
|---------|-------------|---------|----------|
| Default | | | 10.1.0.1 |

system device name get

The current device name is CT100B.

system mode get

Current system mode is: active