



**Smart Network. Smart Business**



# Alteon ADC Virtual Lab Training Manual

OS v32.x

**ALTEON ADC [PROFESSIONAL] LAB MANUAL**

Course 500-100

Document ID / Version: 2018 Dec 5

Copyright © 1998-2018

**NOTICE of RIGHTS**

All rights reserved. The copyright and all other intellectual property rights and trade secrets included in this guide are owned by Radware Ltd. The document is provided to Radware customers for the sole purpose of obtaining information with respect to the installation and use of the Radware products described in this document and is not used for any other purpose.

The information contained in this document is proprietary to Radware. It is strictly forbidden to copy, duplicate, reproduce, transmit, or disclose this document or any part thereof in any form by any means, electronic, mechanical, photocopying, recording, or otherwise, with the prior express written consent of Radware.

**NOTICE of LIABILITY**

The information in this document is distributed on an "as is" basis, without warranty, and is subject to change without notice. Reasonable efforts have been taken to ensure accuracy of the information provided in the preparation of the book. Radware shall have no liability to any person or entity with respect to any loss or damage caused or alleged to be caused directly or indirectly by the instructions contained in this document or by the computer software and hardware products described in it.

Published in the United States of America.

Radware Ltd.

575 Corporate Drive

Mahwah, NJ 07430

(201) 512-9771

[www.radware.com](http://www.radware.com)

## How TO USE THIS MANUAL

Radware Technical Training modules and manuals are designed to convey the most information to the broadest audience by employing auditory, visual, and experiential elements.

Training delegates are strongly encouraged to view ONE Alteon Level 1 training module at time -- then immediately complete the corresponding hands-on lab. Do not wait to view ALL training modules before beginning hands-on labs – but instead, use a “learn it, try it” pattern for learning.

This manual is designed using Just-in-Time (JIT) learning methodology. Buttons are provided (as shown below) so delegates can immediately access essential information needed to complete a lab-task.

When delegates are asked to perform a lab-task, essential information is immediately provided. Accessing this information is optional; delegates are encouraged to try to recall previous learning, then try the task -- and only access essential information if necessary.

Click SHOW button to display various information for help (i.e. screen shot).

Click HINT button for bits of help.

Click WEB button to display information on graphical user interface or other browser-based help.

Click Demo button to display video demonstration to complete procedure.

Click CLI button for help with the commands used with the command line interface.

# TABLE OF CONTENTS

---

- To navigate this document, click on any heading shown here.
- To return to this Contents page, click “Go to Contents” in the footer of any page.

<b>INTRODUCTION TO LAB</b>		<b>MONITORING WITH DPM</b>
Lab Configuration Details - Alteon VA	6	TASK: Use DPM on Alteon
TASK: Connect to lab devices	8	TASK: DPM - Report Granularity
<b>INITIAL SETUP CONFIGURATION</b>		<b>APPENDIX</b>
TASK: Reconnect and explore	13	Validate your Configuration
TASK: Reset and set up Alteon	14	Lab Topology - Alteon VA (printable)
TASK: Check your configuration	15	Lab Topology - Alteon HA (printable)
<b>SWITCHING &amp; ROUTING</b>		Create VLAN using Web GUI
TASK: Configure basic setup	19	Create Server Group using Web GUI
<b>BASIC SLB CONFIGURATION</b>		Add IP Interface using Web GUI
TASK: Configure basic SLB	23	Create Virtual Server using Web GUI
<b>SLB PERSISTENT WITH COOKIE</b>		Define Real Servers using Web GUI
TASK: Persistent SLB	28	Save Configuration using Web GUI
		Configuration Files (to copy/paste)
<b>SSL SERVICES</b>		62
TASK: SSL acceleration	32	
<b>HIGH AVAILABILITY</b>		
Lab Configuration Details - Alteon HA	36	
TASK: Configure Setup on Active (A)	38	
TASK: Configure Setup on Backup (B)	40	
TASK: Configure HA on Device A & B	42	
TASK: HA Synchronization	44	

# INTRODUCTION TO LAB

## **CONNECTION TO VIRTUAL LAB DEVICES**

### **Objectives**

After viewing module “**Intro to ADC**” (optional) and “**Technical Overview**” then completing this lab, you should be able to:

Recognize Alteon virtual lab environment set up.

- Know the preferred method for direct access of Alteon.
- Understand what equipment is needed to complete Alteon Labs.
- Study the Lab Configuration Details - Alteon VA “*Remote Lab - Alteon VA*.”

### **Overview**

This manual is designed with buttons for “just-in-time” (JIT) help to complete hands-on configuration. Use this manual in conjunction with Alteon Level 1 Professional Training Modules. AFTER viewing ONE Alteon Professional module, complete the corresponding Alteon lab. Return to training modules, as needed, for review, explanation, and clarification of basic information. For more instruction on this manual, see *How to use this manual*. [Click blue-dashed area as a hyperlink.]

### **INTRO TO VIRTUAL LAB SET UP**

Your Alteon VA lab is already set up physically **with all required cables and connections**. The web servers and Team-PC has been configured and set up.

- a. Review lab topology in Lab Configuration Details - Alteon VA [Click blue-dashed area as a hyperlink].
- b. For ease, print this (blank) topology and write your Team ## information in the blanks as a reference.[Click blue-dashed area as a hyperlink.]

## Lab Configuration Details - Alteon VA

**Remote Lab – Alteon VA**

**Lab Connection Information**

USA	njlab1.radware.net
Germany	delab1.radware.net
Japan	jplab1.radware.net

For VNC display select **FULL** color

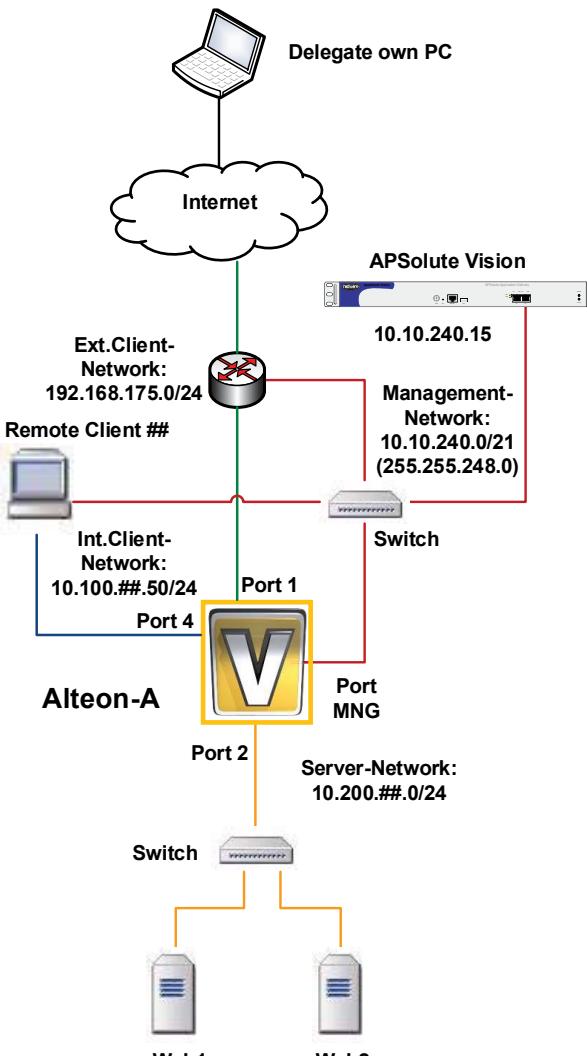
**Remote-Client**  
VNC: 22##  
Password: radware

**Management port:**  
Remote Serial (VNC): 25## (A)  
Remote Secure-SSH: 26## (A)  
Remote Secure-WBM: 27## (A)

**Load Balancing:**  
Remote VIP port 80: 24##  
Remote VIP port 443: 23##

**APSolute Vision**  
<https://njvision1.radware.net>  
<https://devision1.radware.net>  
<https://jpvision1.radware.net>  
Username: AL-Team##  
Password: radware

**## = team number**



**Alteon A Information**

MNG	10.10.242.##/21
MNG-GW	10.10.240.1

**Ext. Client network**  
port 1 → Vlan 11  
if-1 = 192.168.175.## /24 Vlan 11

**Server network**  
port 2 → Vlan 14  
if-2 = 10.200.##.## /24 Vlan 14

**Int. Client network**  
port 4 → Vlan 24  
if-4 = 10.100.##.1 /24 Vlan 24

**Gateway 1** = 192.168.175.254

**Load Balancing**  
PIP on port 1: 10.200.##.70  
VIP = 192.168.175.50 + ##  
Web1 = 10.200.##.100  
Web2 = 10.200.##.200

Your virtual lab consists of:

Virtual Lab Setup	
(1)	Alteon VA (Active = A)
(1)	Alteon VA (Backup = B)
(1)	Management Workstation (Virtual Team-PC)
	Use Application Menu for tools & utilities
	Use TFTP and preconfigured Syslog Server
(2)	Web Servers (Web1, Web 2)

## LAB PREP: Prepare local computer

 **IMPORTANT:** If you haven't already been assigned an Alteon Lab Team##, email your RadwareTechnician at [radwarevirtuallab@radware.com](mailto:radwarevirtuallab@radware.com)

To begin this lab, you should have installed on your local computer:

Your local computer with	
VNC Viewer	For Radware Lab - remote access software
Web Browser	Java-enabled for GUI
* PUTTY	Terminal emulator software - SSH, Telnet

 **NOTE:** \*Radware Trainers suggest using PuTTY to make management port connection (CLI) -- because PuTTY is a free, open-source terminal emulator software that supports several network protocols including SSH, Telnet and more.

## LAB TASK SUMMARY

Here is a summary of what you'll be completing in this lab:

### △ Connect to lab devices

- Connect to Alteon console port
- Connect to Alteon management port
- Connect to Alteon's web-based management (web-GUI)
- Connect to Radware's Lab Management Workstation (Team-PC)

## TASK: Connect to lab devices

### 1. Connect to Alteon console port (Command-line interface or CLI).

 **IMPORTANT:** In your business-setting (on your own physical device), this console port connection is achieved directly using the DB9 cable.

- a. In Radware's virtual lab, console port connection is achieved via VNC Viewer on port 25## <URL:25##>.

▼ Open your local VNC Viewer:

- i. Enter your lab global URL

- Europe Lab = delab1.radware.net
- APAC Lab = jplab1.radware.net
- Americas Lab = njlab1.radware.net

- ii. After URL, type : **25** and your Team## <URL:25##>.

- iii. Click **Connect** to open session ( or hit ENTER).

- b. Log into Alteon: username / password = admin.

 **NOTE:** Radware Labs use AlteonOS v32.+ -- which ENABLES remote access via SSH and HTTPS by default. If your business-setting Alteon uses OSv30.0 or older, you must manually enable SSH / HTTPS separately via Alteon console port whenever you reboot.

- c. *If your screen is black* -- you may need to Troubleshoot VNC settings. [Click blue-dashed area as a hyperlink.]

 **IMPORTANT:** We will walk through each port connection as follows. If you have problem connecting to your Alteon Team##, check your firewall settings. Be sure your firewall has OPEN Destination TCP Ports as follows:

OPEN THESE PORTS ON YOUR FIREWALL		
System		Destination Port
Console Port Connection to Alteon	VNC	25## (active) 250## (backup)
SSH Session to Management Port	SSH	26## (active) 260## (backup)
Secure Web-based Management (WEB-GUI) Connection	HTTPS	27## (active) 270## (backup)
Your Team-PC	VNC	22##
Local-direct access to configured VIP servers	HTTP    HTTPS	24## 23##

## 2. Connect to Alteon management port (CLI).

 **IMPORTANT:** The management port is used exclusively to manage the Alteon through an out-of-band Ethernet connection and through web-based management.

 **NOTE:** While it is not recommended, management of the Alteon VA is also possible through in-band connections on all data ports via Telnet, SSH, HTTP or HTTPS.

- a. In Radware's virtual lab, management port connection is achieved in an SSH session.  
Use PuTTY on port 26##.

▼ From your local PC, open PuTTY (terminal emulator software).

- i. Select **Connection Type: SSH**
- **Category:** Terminal > Keyboard > TheBackspaceKey to Control-H
- **Category:** Window > Translation > ReceivedDateAssumed [or RemoteCharacterSet] to CP437
- ii. Enter **Host Name** for your assigned virtual lab device. This is the global URL for your assigned device:
  - Europe Lab = delab1.radware.net
  - APAC Lab = jplab1.radware.net
  - Americas Lab = njlab1.radware.net
- iii. Add **Port 26##** (Team## as two digits). Password = radware.

☐ TIP: **Name and save** this SSH session for easy repeat.

iv. Click **Open** button.

b. Log into Alteon: username / password = admin.

### 3. Connect to Alteon's web-based management (web-GUI).

a. On your local computer, open a secure (https)browser connection:

i. Enter `https://<URL:27## /webui/default.html>`

ii. Accept Radware as a secure site (Add Exception).

b. Log into Alteon: username / password = admin.

### 4. Connect to Radware's Lab Management Workstation (Team-PC).

☐ **IMPORTANT:** This is your Team-PC. It is used as the Syslog server and TFTP server to save configuration files during labs. Includes other tools: TFTP for saving your configuration files.

a. In Radware's virtual lab, this connection is made via VNC Viewer on port 22##  
`<URL:22##>`.

▼ Open your local VNC Viewer:

i. Enter your lab global URL

- Europe Lab = delab1.radware.net
- APAC Lab = jplab1.radware.net
- Americas Lab = njlab1.radware.net

ii. After URL, add : 22 and your Team## `<URL:22##>`.

iii. Click **Connect** to open session ( or hit Enter).

## TROUBLESHOOT VNC VIEWER SETTINGS

If your VNC screen is black or if Viewer is not displaying properly, try the following:

a. Verify you are using the correct global URL:

- Europe Lab = delab1.radware.net
- APAC Lab = jplab1.radware.net
- Americas Lab = njlab1.radware.net

- b. For a new session, you may need to hit any key (i.e. down arrow) to see the screen.
  - The PC disables the display after a short period.
- c. Check the settings on your VNC viewer.
  - Try increasing quality to include FULL COLORS.
  - Be sure '**Adapt to Network Speed**' is UNCHECKED.
  - Be sure '**Always Use Best Available Color Quality**' is CHECKED.
- d. If these suggestions do not work for you, try using **TightVNC** instead of **RealVNC**.

# INITIAL SETUP CONFIGURATION

## ALTEON MANAGEMENT

### Objectives

After viewing module entitled “**Setup Configuration**” and completing this lab, you should be able to:

- Access device for command line interface.
- Access device for web-GUI.
- Set up management interface.
- Reset the device to factory default.
- Customize the prompt for each switch.



### Overview

In this virtual, hands-on Radware Lab you'll make the initial connection to the Alteon ADC (Application Delivery Controller).

### THREE WAYS TO CONNECT TO AN ALTEON ADC

In your business-setting, you may normally connect to the Alteon in one-of-three ways:

1. Connect to command line interface (CLI): CLI is a built-in, text-based menu system for access. This is the most direct method for configuring Alteon.
  - i. **Console port serial connection using SSH / Telnet** (running terminal emulation software i.e. PuTTY).
  - ii. **Management port connection** (out-of-band gigabit ethernet cable) used exclusively for managing Alteon
  - iii. **Telnet network connection** from any workstation connected to the network provides same access as console port connection.

2. Connect using secure, web-based management (WBM) -- accessing Alteon web-GUI which uses Java-enabled browser via https.
3. Connect using Radware's APSolute Vision (optional separate license).

## LAB TASK SUMMARY

Here is a summary of what you'll be doing in lab:

△ **Reconnect and explore**

- Reconnect to Alteon web-GUI
- Reconnect to Alteon CLI
- Reconnect to your Team-PC

△ **Reset and set up Alteon**

- Reconnect to Alteon console port (CLI)
- Reset (reboot) Alteon
- Set up management interface
- Customize prompt
- Lengthen idle timeout
- Save Configuration

△ **Check your configuration**

- Reconnect to web-GUI
- Disable VLAN 1

## TASK: Reconnect and explore

1. Reconnect to Alteon's web-GUI using a browser on your local computer (27##).

☐ TIP: Alteon login: username & password = admin.

- a. Explore web-GUI environment.
  - i. Go to > CONFIGURATION perspective

- ii. Select different BLUE navigation options.

- Notice different options/choices.
- See different display/tab changes.

☐ NOTE: Any changes you make will soon be reset so no problems will be caused to your lab exercises.

**2. Reconnect to Alteon's CLI using VNC Viewer (26##).**

- a. Explore CLI menu navigation.

**3. Reconnect to your lab Team-PC using VNC Viewer (22##).**

 **IMPORTANT:** Your Team-PC is used as the Syslog server and TFTP server to save configuration files during labs.

- a. Explore Team-PC tools. Note IP address.

## TASK: Reset and set up Alteon

### SETUP A: CONNECTION

#### Setup A Connection

**1. Reconnect to Alteon console port (CLI )using VNC Viewer (25##).****2. Reset (reboot) Alteon to factory default settings.**

 TIP: Wait approximately 5 seconds, then log into the Alteon.

### SETUP B: MANAGEMENT ACCESS

#### Setup B Management Access

**3. Set up the management interface.**

- a. Set TFTP to use management port.

 TIP: Before you can configure a static address, DHCP must be disabled.

 NOTE: APPLY and SAVE changes.

- b. **After Alteon reset**, enable remote access to management port. Radware Labs must enable only SNMP (when using Vision).

 **NOTE:** Radware Labs use AlteonOS v32+. Starting with AlteonOS v30.0+, SSH and HTTPS are enabled by default. If your business uses an older version, you must enable SSH and HTTPS in addition to SNMP.

- c. **After Alteon reset**, confirm remote access by trying SSH and HTTPS.

## SETUP C: SECURE THE DEVICE

### Setup C Secure the Device

#### 4. Customize the prompt for your Alteon.

 TIP: Use Team## as string name; then activate (enable) the customized prompt.

#### 5. Lengthen Alteon idle timeout.

 TIP: Set idle time to 9999 minutes so the device does not idle out. APPLY and SAVE.

#### 6. Save your configuration.

 TIP: EASY --> APPLY and SAVE.

## TASK: Check your configuration

#### 1. Re-connect remotely to Alteon via web-GUI to check your configuration.

##### a. Go to *Configuration* -> *System*

- Verify management interface settings you configured previously.

##### b. Go to *Configuration* -> *System* -> *Management Access* -> *Management Ports*

- Verify management ports.

- c. Go to *Configuration* -> *System* -> *Management Access* -> *Management Traffic Routing*
  - i. Verify management traffic routing
- d. Go to *Configuration* -> *System* -> *SNMP*
  - i. Verify SNMP settings

## 2. Disable VLAN 1



**IMPORTANT:** Be sure to disable VLAN 1 before continuing in Radware's lab exercises.

# SWITCHING & ROUTING

## STANDARD LAYER 2 AND LAYER 3 SETUP

### Objectives

After viewing module entitled “**Switching & Routing**” and completing this lab, you should be able to:

- Set up Alteon to operate as a router: configure VLANs
- Define IP interfaces.
- Set up a default gateway.
- Back up (export) your configuration.
- Modify and import your configuration.



### Overview

In this lab, you will set up the switching and routing for Layer 2 and Layer 3 of the OSI Model.

You will save this configuration as STANDARD SETUP for your virtual lab configuration. You will reuse this STANDARD SETUP configuration throughout the training lab exercises.

After completing standard setup configuration, you should know how to enable, apply, and save your settings for future use. Remember to use this **EASY** acronym to help correctly save your work. Command-line interface (CLI) is **EASY** to use!

- E = Enable
- A = Apply
- S = Save
- Y = Yes to confirm the save



## REVIEW COMPONENTS FOR SETUP

Alteon Training module for basic setup introduced the components for Alteon set up:

1. Configure Ports
2. Set up VLANs
3. Define Interfaces
4. Set Default Gateway

## LAB PREP: Access Alteon

Before you begin this lab you should:

- a. Access Alteon and login.

## LAB TASK SUMMARY

Here is a summary of what you'll be doing in lab:

△ **Configure basic setup**

- Setup Layer 2 VLANS
- (Opt) L2 Advanced Configuration
- Define L3 IP interfaces
- Set default gateway

△ **Validate your configuration**

## TASK: Configure basic setup

### STEP 1: L2 SETUP VLANS

#### Step 1: L2 Setup VLANs

##### 1. Configure Layer 2 (L2) VLANs.

- Set up Alteon to operate as a router.

Configure L2 VLANs	
Physical Port	VLAN ID
Port 1	VLAN 11
Port 2	VLAN 14
Port 4	VLAN 24

### STEP 2: (OPT) ADVANCED L2 CONFIG

#### Step 2 (opt) : Adv L2 Configuration

##### 2. Turn off Spanning Tree Group (STG 1).

 TIP: Up to 16 different Spanning Tree Groups.

### STEP 3: L3 DEFINE INTERFACES

#### Step 3: L3 Define Interfaces

Configure L3 IP interfaces		
IF ID	IP Address	VLAN ID
IF 1	192.168.175.## / 24	VLAN 11
IF 2	10.200.##.## / 24	VLAN 14
IF 4	10.100.##.1 / 24	VLAN 24

- Mask = /24 is 255.255.255.0

☐ TIP: Try two methods for CLI; try multi-line option or try single-line/stacked CLI option.

## STEP 4: L3 SET DEFAULT GATEWAY

### Step 4: L3 Set Default Gateway

#### 4. Set default gateway 192.168.175.254.

☐ TIP: Gateway 1-4 for all VLANs.

☐ **IMPORTANT:** Apply and save configuration.

## VALIDATE YOUR CONFIGURATION

☐ **HINT:** Check - Test - Export - Reset - Import

#### 1. Check the configuration.

#### 2. Test device connectivity.

##### a. Ping all devices

☐ **IMPORTANT: If all Pings fail** for Lab ONLY, you may need to reboot your device after creating a default gateway. Apply and save your configuration.

#### 3. Export (save) the configuration.

☐ **IMPORTANT:** Always YES = "Include Private Keys" so the configuration can be imported later.

##### a. May use CLI command to export: name file STANDARD SETUP.

##### i. Export configuration using CLI "put config" command and TFTP server.

##### ii. Use IP address of the Workstation of the management network = 10.10.242.2# #.

☐ **IMPORTANT:** Reconnect to Team-PC to see that STANDARD SETUP file exported (saved) there.

b. May use web-GUI to export: name file STANDARD SETUP.

c. Modify, rename, and import configuration.

i. Use any plain-text editor to modify your configuration.

ii. Add new interface #100 with IP 192.168.250.100.

iii. Save modified configuration as NEW CONFIG.

 **NOTE:** Apply and save configuration.

#### 4. Reset (reboot) your Alteon device.

a. Reset device to factory default settings.

i. Save management network? = YES.

b. After reset, enable remote access to management port. {Radware labs enable SNMP only -- used for APSolute Vision.)

 **NOTE:** Radware Labs use AlteonOS v30.5+ -- which ENABLES remote access via SSH and HTTPS by default. If your business-setting Alteon uses OSv30.0 or older, you must manually enable SSH / HTTPS separately.

c. After reboot, set TFTP to use management port.

i. Configure static IP address of Team-PC as 10.10.242.2##. DHCP must be disabled before a static address can be configured.

#### 5. Import modified configuration.

a. Check differences between the configurations.

 **TIP:** Use CLI `diff`

b. Delete new interface #100 with IP you added.

 **TIP:** Remember to APPLY and SAVE changes.

# BASIC SLB CONFIGURATION

## ***BASIC SERVER LOAD BALANCING SETUP***

### **Objectives**

After viewing module "*Introduction to SLB*" and then completing this lab, you should be able to:

- Configure basic server load balancing (SLB).
- Export (save) SLB configurations to a file.
- Validate your configuration with test-traffic to web servers.



### **Overview**

In this lab we configure the Alteon to support basic server load balancing. We configure basic server load balancing (SLB) by setting up Layer 4 real server and binding them into a group.

We also bind the load balancing metric and health check to the server group. Then we configure the virtual server and assign a service -- and bind that the server group. We're all set to load balance.

### **LAB PREP: Restore Standard Setup**

Before you begin this lab:

- a. You should have successfully completed routing and switching STANDARD SETUP configuration.
- b. Access Alteon management port and login.
  - i. Import STANDARD SETUP configuration -- else be sure it is already the Alteon configuration.
- c. Verify your current STANDARD SETUP configuration is working before going forward.

**HINT:** Check - Verify.

## LAB TASK SUMMARY

Here is a summary of what you'll be doing in lab:

△ **Configure basic server load balancing**

- Define real servers
- Create server group
- Bind health check to the group
- Create virtual server and bind to the group
- Define virtual service

△ **Validate your configuration**

## TASK: Configure basic SLB

### STEP 1: DEFINE REAL SERVERS

**Step 1: Define real servers (ID & IP)**

1. Define real Server1 and Server2.

Configure Real Servers	
Real Server ID	Server IP Address
Server1	10.200.##.100
Server2	10.200.##.200

☐ NOTE: Real server ID = up to 32 alpha-numeric characters, case-sensitive, NO SPACES.

☐ TIP: Try Method A using multi-line CLI option.

☐ See Method B single-line / stacked CLI option.

## STEP 2: CREATE SERVER GROUP

Step 2: Create server group (add servers)

### 2. Create server group. Use server group ID=1.

- a. Add *Server1* and *Server2* to the group.
- b. Set metric for the group to *roundrobin*.

## STEP 3 (OPT): SET ADV HEALTH CHECK

Step 3 (opt): Set Advanced Health Checks

### 3. Bind health check = ICMP to the group.

 NOTE: All real servers for a specific service belong together in a group.

## STEP 4: CREATE VIRTUAL SERVER

Step 4: Create virtual server

### 4. Create virtual server ID =1.

Virtual Server Settings	
Virtual Server	VIRT ID = 1
VIP Address	192.168.175.%%  NOTE: %% = ## + 50

- a. Configure VIRT at 192.168.175.%%.

 NOTE: See VIP where %% = sum of Team## + 50.

## STEP 5: DEFINE VIRTUAL SERVICE

### Step 5: Define virtual service

#### 5. Define virtual service as http port 80 and bind to the group.

- a. Force connection through Proxy IP in the http service.
- b. Bind to server group ID = 1.

Virtual Services	
Service	http (port 80)
Proxy IP	10.200.##.70 / 32
Group	Group ID = 1

- ☐ TIP: This is the entry or termination IP address for a specific service -- standalone Alteon. For Radware Lab, forcing through proxy IP ensures connection through the PIP -- no matter if connection is made directly, via Port 24## or Team-PC.
- ☐ **IMPORTANT:** Radware Labs use AlteonOS v32.+. Starting with AlteonOS v30.0+, **server load balancing, port client processing, server processing, and proxy processing** are enabled by default. If your business uses an older version, you must enable these features separately -- on each respective port.

## VALIDATE YOUR CONFIGURATION

- ☐ **HINT:** Check - Test - Stats - Export

#### 1. Check configuration.

- ☐ TIP: Did you enable, apply, and save -- **EASY**

#### 2. Test connectivity.

- a. Test that web servers are operating (UP).

- ☐ TIP: If messages not visible, try turning ON message display log.

### 3. Verify configuration by generating test-traffic to your web servers.

 **IMPORTANT:** You will need to configure the VIP to your lab server group. This is your Team##. Use it to generate test-traffic within the lab to validate your lab configuration.

- a. Connect to your web server(s) from your local computer (directly). Browse to `http://<LabURL>:24##`.

- b. If you cannot connect to your web server(s) *directly*, then go to Team-PC to connect *indirectly*. On Team-PC, browse to your VIP.

- c. Accept Radware as a secure site -- add exception.

 **NOTE:** You should see a response that you reached Server1 or Server2. You may need to open a new browser window to see load balancing working.

### 4. View statistics on your virtual server connection.

- a. Generate additional test-traffic to servers and view changes in virtual server statistics.

- i. Open new browser window to your VIP several times to generate test-traffic.
  - ii. Return to the Alteon CLI and notice changes to the Alteon statistics.

 **TIP:** In the Alteon CLI, press the up-arrow key to repeat previous command.

- b. Clear statistics on SLB table; then repeat Stats view.

### 5. Export configuration. Name this **BASIC SLB CONFIGURATION**.

 **TIP:** Be sure clearly name and identify your file on Team-PC.

# SLB PERSISTENT WITH COOKIE

## ***SLB USING LAYER 3 AND LAYER 4 PERSISTENCY***

### **Objectives**

After viewing module entitled “*Persistence with Insert Cookie*” and completing this lab, you should be able to:

- Configure IP persistence by using hash or minmisses.
- Configure L7 cookie persistence using passive, rewrite or insert mode.

### **Overview**

When configuring a load-balanced service, one important issue is dealing with information that must be maintained across multiple requests in a user’s session. To send all requests in a user session consistently to the same backend server is known as persistence or stickiness.

Persistent server load balancing uses Layer 3 and Layer 4 persistency. Layer 3 handles only IP addresses, hash or minmisses are used as the metric.

Layer 7 persistency depends on the application. We use HTTP with passive cookies, cookie rewrite, and cookie insert to provide persistence.

### **LAB PREP: Restore Basic SLB Setup**

Before you begin this lab:

- a. You should have successfully completed BASIC SLB configuration.
- b. Access Alteon management port and login.
  - i. Import BASIC SLB configuration -- else be sure it is already the Alteon configuration.
- c. Verify your BASIC SLB configuration is properly working before going on.

 **HINT:** Check - Verify.

## LAB TASK SUMMARY

Here is a summary of what you'll be completing in this Persistent SLB Lab:

### △ Persistent SLB

- Set group metric to PHash
- Change metric to Roundrobin
- Change server cookie
- Enable passive cookie
- Revert rport back
- Configure to insert session cookie

### △ Validate your Configuration

## TASK: Persistent SLB

 **IMPORTANT:** To begin this lab, enable **Direct Access Mode** (DAM) globally.

### 1. Set the group metric to PHASH.

- a. Verify this configuration change.
  - i. Generate test-traffic and verify all persistent connections to a single server even after session table expires (60 seconds).

### 2. Change group metric to Round Robin.

### 3. Currently, the web server with cookie is on real port 88. Change the virtual server rport value to 88.

### 4. Clear the session table and clear the SLB statistics.

- 5. Enable passive cookie-based persistence on the virtual server service.**
  - a. Enable the VIRT to track passive cookies.
  - b. Test the configuration.
    - i. First disable all cookies in the browser and notice sessions moving between two servers.
    - ii. Then enable cookies in the browser and notice sessions go to the same server.
    - iii. Close all browsers and time out of the session table (or clear the session table). Notice the connection to a new server (unlike phash).
- 6. Revert virtual server report back to port 80 (server has no cookie).**
- 7. Configure virtual server to insert a session cookie.**
  - i. Optionally you can insert a time duration cookie (expires by date or expires by time).

## VALIDATE YOUR CONFIGURATION

 HINT: Check - Export

- 1. Inspect the cookie inserted.**
  - a. Connect to VIP using Firefox with Firebug or Live HTTP Headers plugin.

 NOTE: Notice the cookie inserted by the Alteon under the cookie session. Cookie rewrite/insert upgrade in v29.5.1 -- Generates a persistency entry (p-entry) in the session table.
- 2. Compare the inserted cookie (as previous) with Alteon cookie table.**

 TIP: Use CLI operations menu.

3. Export configuration as a backup. Name it **BACKUP PERSISTENT SLB LAB**.
4. In preparation for the next lab, import (get) **BASIC SLB CONFIGURATION**.

# SSL SERVICES

## ***SECURE SOCKET LAYER ACCELERATION & OFFLOADING***

---

### **Objectives**

After viewing module entitled “SSL Services” and completing this lab, you should be able to:

- Enable and configure SSL services on Alteon.
- Create Certificate and SSL policy.

## **Overview**

In this lab, we enable SSL -- Alteon’s services for acceleration and offloading capabilities. Secure Sockets Layer (SSL) is a security layer that can be added to various communication protocols. SSL performs encryption, decryption, and verification of transmissions between clients and servers

SSL relieves the back-end servers of tasks -- thus enabling the back-end servers to maximize their performance and efficiency. This results in faster server response times and increased server capacity to handle more users that are concurrent.

## **LAB PREP: Restore Basic SLB**

Before you begin this lab:

- a. You should have successfully completed BASIC SLB configuration.
- b. Access Alteon management port and login.
  - i. Import BASIC SLB configuration -- else be sure it is already the Alteon configuration.
- c. Verify your BASIC SLB configuration works properly before continuing.

 **HINT:** Check - Verify.

## LAB TASK SUMMARY

Here is a summary of what you'll be doing in lab:

△ **SSL Acceleration**

- Enable SSL globally
- Create a certificate
- Define SSL Policy
- Associate to virtual service

△ **Validate your configuration**

## TASK: SSL acceleration

 **IMPORTANT:** Enable SSL globally to begin this lab.

### STEP 1: CERTIFICATE MANAGEMENT

**Step 1: Certificate Management**

1. Create and generate a self-signed server certificate for a service (key will be added).
  - i. Certificate ID = Team##
  - ii. Certificate Name = MyTeam##Cert
  - iii. Certificate Common Name = www.team##.com (where ## = your team number).
  - iv. For any other values, use default settings or as desired

 **NOTE:** Verify that "**Self signed certificate, certificate signing request and key added**".

## STEP 2: SSL POLICY DEFINITION

### Step 2: SSL Policy Definition

#### 2. Define SSL Policy -- which will govern SSL behavior.

- i. SSL policy ID = MYPOLICY
- ii. SSL policy Name = EasySSLPolicy
- iii. cipher = main.

 TIP: Remember to enable the policy.

## STEP 3: VIRTUAL SERVICE ASSOCIATION

### Step 3: Virtual Service Association

#### 3. Associate to virtual service.

- a. Associate HTTPS service (defined).
- b. Bind Certificate to service
- c. Bind SSL Policy to service
- d. Add PIP (proxy IP) 10.200.##.70 on service 443 https.

 TIP: Remember to apply configuration changes.

## VALIDATE YOUR CONFIGURATION

 HINT: Check - Verify - Export

#### 1. Check SLB configuration.

## 2. Verify configuration by generating test-traffic to your servers.

- a. Connect to your server(s) from your local computer (directly) by browsing to `http://<LabURL>:24##`.
  - i. If you cannot connect directly, try this.
- b. View statistics on your virtual server connection -- then clear statistics.

## 3. Enable Application Trace Log for SSL.

 TIP: Application services tracelogging may cause performance impact on Alteon traffic processing capabilities. Be sure to disable when done.

- a. Connect using secure SSL `https://<LabURL>:23##`.
- b. Generate test traffic by accessing the https server page several times.
- c. Export data file to your Team-PC. Turn on 3CD and listen to TFTP service.
- d. Extract the file and view it with wordpad.

 TIP: There is a separate data log file for each SP.

## 4. Export configuration.

- a. Name exported file: `SSL_Services`.

# HIGH AVAILABILITY

## **CONFIGURING THE REDUNDANT NETWORK**

### **Objectives**

After viewing module entitled “*High Availability*” and completing this lab, you should be able to:

- Configure Active and Backup Alteon devices for High Availability failover.

### **Overview**

In this lab you will set up a redundant network for high availability. The single-switch configuration is enhanced by a second switch to provide High Availability (HA) based on enhanced configuration on Alteon OS v30.2 (or higher). The legacy-mode high availability (VRRP) is supported in software v30.1 (and earlier). For more information on VRRP, refer to Alteon Application Guide.

You'll configure HA for active Alteon (Active = A) and backup Alteon (Backup = B) devices. High availability is maintained as follows: if the active device fails and no longer passes traffic, the backup device takes over. This minimizes downtime on a critical network.

To complete lab exercises, you should be assigned two Alteon VA instances (devices): Active = A and Backup = B. If you were not assigned two instances (devices), please contact [virtuallab@radware.com](mailto:virtuallab@radware.com).

This High Availability Lab uses the diagram Lab Configuration Details - Alteon HA. All network cables are connected as depicted. The Team-PC (local Workstation running VNC viewer or PuTTY) or web server in this lab is already preconfigured. For technical support, ask your local trainer or email Radware Technical support at [virtuallab@radware.com](mailto:virtuallab@radware.com).

## Lab Configuration Details - Alteon HA

**Remote Lab – Alteon VA - HA**

**Lab Connection Information**

USA      njlab1.radware.net  
Germany    delab1.radware.net  
Japan     jplab1.radware.net

For VNC display select **FULL** color

**Remote-Client**  
VNC: 22##  
Password: radware

**Management port:**  
Remote Serial (VNC): 25## (A) 250## (B)  
Remote Secure-SSH: 26## (A) 260## (B)  
Remote SecureWBM: 27## (A) 270## (B)

**Load Balancing:**  
Remote VIP port 80: 24##  
Remote VIP port 443: 23##

**APSolute Vision**  
<https://njvision1.radware.net>  
<https://devision1.radware.net>  
<https://jpvision1.radware.net>  
Username: AL-Team##  
Password: radware

**Alteon A Information**

**MNG**      10.10.242.###/21  
**MNG-GW**    10.10.240.1

**External Client network**  
port 1 → Vlan 11  
if-1 = 192.168.175.1## /24 Vlan 11  
Peer IP = 192.168.175.2## /24  
Gateway 1 = 192.168.175.254

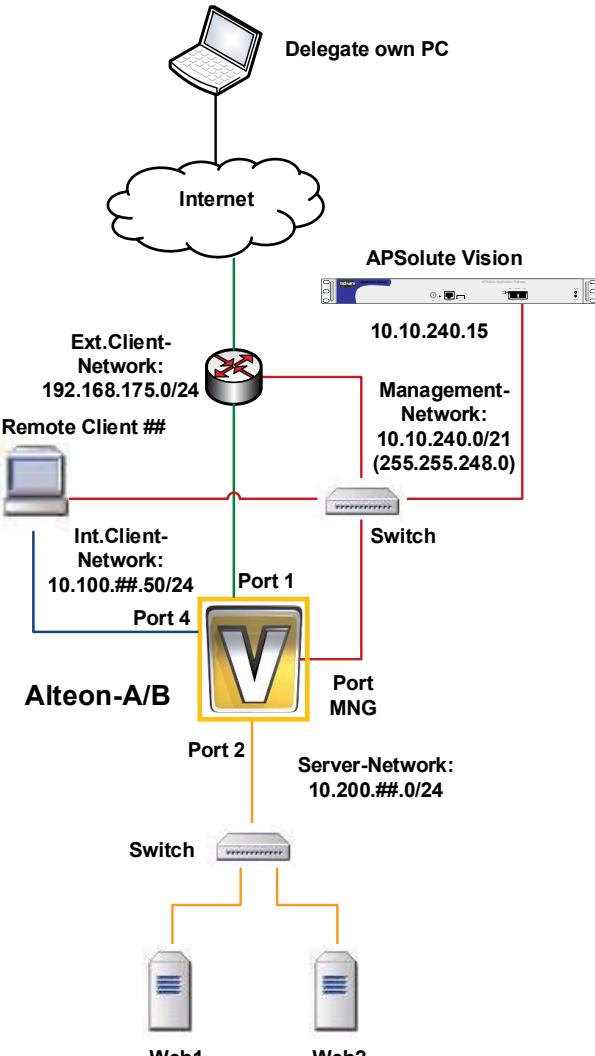
**Server network**  
port 2 → Vlan 14 →  
if-2 = 10.200.##.254 /24 Vlan 14  
Peer IP = 10.200.##.253 /24

**Internal Client network**  
port 4 → Vlan 24  
if-4 = 10.100.##.254 /24 Vlan 24  
Peer IP = 10.100.##.253 /24

**Floating IP Addresses**  
192 . 168 . 175 . ##  
10 . 200 . ## . ##  
10 . 100 . ## . 1

**Load Balancing**  
PIP   = 10.200.##.70  
VIP   = 192.168.175.50+##  
Web1 = 10.200.##.100  
Web2 = 10.200.##.200

**## = team number**



**Alteon B Information**  
For redundancy lab

**MNG** = 10.10.242.1##/21

IF ID	IP Address	VLAN ID
1	192.168.175.2## / 24	11
2	10.200.##.253 / 24	14
4	10.100.##.253 / 24	24

## LAB PREP: Reset Alteon

Before you begin this lab:

### 1. Review Lab Configuration Details - Alteon HA.

- a. For ease, print this (blank) topology and write your ## information in the blanks:
  - i. ## = Assigned Team number (2-digits)
  - ii. %% = Sum of Team ## + 50

### 2. Reset the Alteon to factory defaults.

 **IMPORTANT:** Keep management port connectivity [yes].

- a. Verify the configuration of management port management IP is correct.

## LAB TASK SUMMARY

Here is a summary of what you'll be completing in this High Availability Lab:

△ **Configure (active) Alteon A:**

- Configure Switching & Routing Basic Setup
- Configure SLB on Alteon A

△ **Configure (backup) Alteon B:**

- Verify Management IP on Device B
- Configure Switching & Routing Basic Setup

△ **Configure High Availability on A**

- Enable HA Switch Mode
- Select advertisement interfaces
- (Opt) Configure Session Mirroring
- (Opt) Configure Failover Trigger

△ **Configure Synchronization for A to B**

## TASK: Configure Setup on Active (A)

### CONNECT TO ALTEON ACTIVE DEVICE A.

 TIP: Active Device A ports = 25##, 26## or 27##

 **REMINDER:** These four steps are the basic setup previously discussed in **SWITCHING & ROUTING STANDARD SETUP** -- Standard Layer 2 and Layer 3 setup.

### SETUP STEP 1: L2 SETUP VLANs

- Configure Layer 2 (L2) on Active Alteon (Device A). Create three VLANs; add ports.

Configure L2 VLANs	
Physical Port	VLAN ID
Port 1	VLAN 11
Port 2	VLAN 14
Port 4	VLAN 24

### SETUP STEP 2 (OPT): ADV L2 CONFIG

- Turn off Spanning Tree Group (STG).

### SETUP STEP 3: L3 DEFINE INTERFACES

- Define Layer 3 (L3) IP interfaces.

- Configure interface IP addresses.

Configure Layer 3 IPs = Alteon A		
IF ID	IP Address	VLAN ID
1	192.168.175.2##	VLAN 11
2	10.200.##.254	VLAN 14
4	10.100.##.254	VLAN 24

- Mask = 255.255.255.0

## SETUP STEP 4: L3 SET DEFAULT GATEWAY

- Set default gateway 192.168.175.254.

 **IMPORTANT:** Apply and save configuration. For Radware Lab only, you may need to reboot your device after creating a default gateway. **Be sure to save configuration.**

## CONFIGURE SLB ON ACTIVE DEVICE A

- Configure Server Load Balancing on Device A.

- Create two servers, add to group, create VIRT with Virtual IP 192.168.175.%%.  
Assign Service 80 HTTP.

 **TIP:** For %% = sum of ## + 50

Configure SLB on Alteon A	
Server1	RIP 10.200.##.100
Server2	RIP 10.200.##.200
VIRT1	VIP 192.168.175.%%
Service	80 HTTP
PIP	10.200.##.69
Group	Group = 1

- Apply and Save configuration changes.

## VALIDATE YOUR CONFIGURATION

 **HINT:** Check - Test

- Check configuration.

## 2. Test device connectivity.

 **HINT:** Ping Default Gateway IP address. Ping Server(s) IP address(es).

a. If all Pings fail, reboot your Alteon device.

 **IMPORTANT:** Apply and save configuration. For Radware Lab only, you may need to reboot your device after creating a default gateway. **Be sure to first save the configuration. Always keep management port connectivity [yes].**

## TASK: Configure Setup on Backup (B)

### CONNECT TO ALTEON BACKUP DEVICE B.

 **TIP:** You must "exit" Device A and establish a new connection with Device B ports = 250##, 260## or 270##

a. Verify the configuration of management port on Backup Alteon Device B has been retained.

 **REMINDER:** These 4 steps are basic setup previously discussed in **SWITCHING & ROUTING STANDARD SETUP** -- Standard Layer 2 and Layer 3 setup.

### SETUP STEP 1: L2 SETUP VLANs

#### 1. Configure Layer 2 (L2) on Backup Alteon. Create three VLANs and add ports.

Configure L2 VLANs	
Physical Port	VLAN ID
Port 1	VLAN 11
Port 2	VLAN 14
Port 4	VLAN 24

### SETUP STEP 2 (OPT): ADV L2 CONFIG

#### 2. Turn off Spanning Tree Group (STG).

## SETUP STEP 3: L3 DEFINE INTERFACES

### 3. Define Layer 3 (L3) IP interfaces.

#### a. Configure IP addresses.

Configure Layer 3 IPs = Alteon B		
IF ID	IP Address	VLAN ID
1	192.168.175.1##	VLAN 11
2	10.200.##.253	VLAN 14
4	10.100.##.253	VLAN 24

#### i. Mask = 255.255.255.0

## SETUP STEP 4: L3 SET DEFAULT GATEWAY

### 4. Set default gateway 192.168.175.254.

 **IMPORTANT:** Apply and save configuration. For Radware Lab only, you may need to reboot your device after creating a default gateway. **Be sure to first save configuration. Always keep management port connectivity [yes].**

#### a. Apply and Save configuration changes.

## VALIDATE YOUR CONFIGURATION

 **HINT:** Check - Test

### 1. Check configuration.

### 2. Test device connectivity.

 **HINT:** Ping Default Gateway IP address. Ping Server(s) IP address(es).

#### a. If all Pings fail, reboot your Alteon device.

 **IMPORTANT:** For Radware Lab only, you may need to reboot your device after creating a default gateway. Save configuration. Keep management port connectivity [yes].

## TASK: Configure High Availability on Device A & B

-  **IMPORTANT:** In this lab, we will synch these HA configuration steps from Device A to Device B -- as a result, we only configure HA on Device A.

### HA PRE-STEP A: DEFINE PEER IPs

Step A: Define Peer IPs

#### CONNECT TO ALTEON DEVICE A.

-  TIP: Active Device A ports = 25##, 26## or 27##

1. Define peer IP address for each interface on Device A.

Define Peer IP for each interface	
	Peer IP Address
IF 1	192 . 168 . 175 . 1##
IF 2	10.200.##.253
IF 4	10 . 100 . ## . 253

-  **REMINDER: VERIFY PEER IPs.** Be sure a Peer IP is set for each interface on Device A. Peer IP address is the configured IP address of the OTHER device (ie. Configured IPs of Device B).

### HA PRE-STEP B: ASSIGN FLOATING IPs

Step B: Assign Floating IPs

2. Assign a floating IP address for each interface on Device A.

Configure Floating IPs	
IF ID	FIP Addresses
1	192 . 168 . 175 . ##
2	10 . 200 . ## . ##
4	10 . 100 . ## . 1

-  **Reminder:** A floating IP address is a virtual IP address that is identical for both devices in the HA pair. It must be on the same subnet as the interface and must be different from any other defined IP.

## HA STEP 1: ENABLE HA MODE

Step 1: Enable HA Mode

### 1. Enable High Availability: Switch Mode.

- a. Set Device A as priority (active) Switch HA.
  - i. Use **Fallback Mode**: Always
  - ii. Use **Preferred State**: Active

## HA STEP 2: SELECT ADVERTISEMENT INTERFACE

Step 2: Select Advertisement Interfaces

### 2. Assign Advertisement interfaces.

- a. Apply and Save configuration changes.

△ HA Step 3: (Optional) Configure Session Mirroring

Step 3 (opt): Configure Session Mirroring

- ▼ Not required for this Lab HA -- but if desired, explore the path to configure session mirroring.

△ HA Step 4: (Optional) Configure Failover Trigger

Step 4 (opt): Configure Failover Trigger

- ▼ Not required for this Lab HA -- but if desired, explore configuring failover trigger(s).

## TASK: HA Synchronization

### Step 5: Configure Synchronization

 NOTE: At this point, both devices should be ready for synchronization.

### 3. Configure synchronization on Active A and Backup B.

 **IMPORTANT:** In this lab, we will synch these HA configuration steps from Device A to Device B -- as a result, we only configured HA on Device A.

#### ENSURE CONNECTION TO ACTIVE A.

 **TIP:** You may still be connected. Active Device A ports = 25##, 26## or 27##

a. Define Peer IP address for Active A

i. Use Peer ID = 1

ii. Use Peer IP address = <10.100.##.253>

 **TIP:** IP Address is for the peer Alteon. Only data ports --not management IP -- are valid for sync. Any interface IP would work BUT of Radware Lab, use the IP address for IF 4 from Backup B.

 **IMPORTANT:** Do not sync at this time.

#### RECONNECT TO BACKUP DEVICE B.

 **TIP:** Backup Device B ports = 250##, 260## or 270##

b. Define peer IP address for to Backup B

i. Use Peer ID = 1

ii. Use Peer IP address = <10.100.##.254>

 **TIP:** IP Address is for the peer Alteon. Only data ports --not management IP -- are valid for sync. Any interface IP would work BUT of Radware Lab, use the IP address for IF 4 from Active A.

 **IMPORTANT:** Do not sync at this time.

#### RECONNECTION TO ACTIVE A.

 **TIP:** Active Device A ports = 25##, 26## or 27##

- c. Enable synchronization on Device A

 **IMPORTANT:** Now sync from Active A to Active B.

## VALIDATE YOUR CONFIGURATION

 **HINT:** Check - Test

- a. Validate your synchronization on Device B.
  - i. Re-connect to Device B.
  - ii. Check current configuration on SLB (server load balancing) -- since this was not originally configured on Device B, it should now be synchronized and SLB configured on Device B.
  - iii. If SLB is configured now configured on Device B, synchronization is valid.
- b. Test the configuration.
  - i. Start a continuous ping from Team-PC machine. Ping 192.168.175.## -c 99999.
  - ii. After testing of High Availability (HA) is complete, use the Ctrl+C keys to stop the continuous ping.
-  **TIP:** Connect to the Terminal (VNC session) of both devices. **Device A = NOTICE HA: HA Switch is now MASTER.**
- c. Check the sync status.
- d. On Alteon A, fail the active Master device by disabling VLAN 11.
  - i. Ensure the **Alteon A** changes to the **State: backup**.
- e. Re-enable VLAN 11 on the active.
- f. Re-check the sync status.

4. Export each configuration file to use as backup. Name files: **BACKUP HA ALTEON A** and **BACKUP HA ALTEON B**.

 TIP: See Configuration Files in Appendix

# MONITORING WITH DPM

## **Service Status View & DPM**

### **Objectives**

After viewing module entitled “*Monitoring with DPM*” and completing this lab, you should be able to:

- Enable APSolute Device Performance Monitoring (DPM on the device).
- Report Granularity on DPM.

### **Overview**

APSolute Vision DPM -- *Device Performance Monitoring* is supported on Alteon OS29.0 and higher. DPM requires an APSolute Vision DPM license. A 30-day evaluation license is available.

When DPM is enabled, the Alteon sends its performance data to APSolute Vision. The data is processed and displayed in the DPM web-interface -- alerts, dashboards, reports (current and historical).

### **LAB TASK SUMMARY**

Here is a summary of tasks for this lab:

△ **Use Device Performance Monitoring**

- Enable DPM on the device
- If needed, enable DAM globally
- If needed, enable DAM on virtual service
- 

△ **DPM - Report Granularity**

- Report with high granularity
- Modify granularity

## TASK: Use DPM on Alteon

Using APSolute DPM (*Device Performance Monitoring*) on the Alteon:

- Enable DPM reporting on Alteon.
- \*Must ensure DAM is enabled globally.
- \*DAM enabled for each virtual service.

\*Not relevant on ADC-VX

### 1. Enable DPM Reporting on the Alteon.

 **IMPORTANT:** Radware Labs use AlteonOS v32.+. Starting with AlteonOS v30.0+, **Direct Access Mode (DAM)** is enabled by default. If your business uses an older version, you must enable features separately -- plus be sure it is enabled on each virtual service.

- a. Ensure that **DAM** is enabled globally.
- b. Ensure **DAM** is enabled for each virtual service.

## TASK: DPM - Report Granularity

 **IMPORTANT:** To access DPM, click on the DPM icon on the top bar of the **ApSolute Vision** window.

By default, statistics are collected per virtual service (throughput, PPS, CPS, and so on).

### 1. To receive reports with higher granularity.

- a. Select an extended reporting level per virtual service.  
 TIP: For example, reporting per real server associated with that service.
- b. Modify the DPM report granularity on Alteon:

# APPENDIX

---

**NOTE:** Appendix has various information and demonstrations referenced by hyperlinks elsewhere in these various Lab Books.

## Validate your Configuration

 TIP: REFER BACK TO THIS SECTION. BECOME EXPERT AT VALIDATION.

### 1. Check configuration.

 TIP: This is a visual check. Look at the configuration to ensure you entered it correctly.

- **diff [diff flash memory]**
- **/cfg/slb/cur [current SLB]**

### 2. Test connectivity.

a. Ping all devices

b. If all Pings fail, reboot your Alteon device.

 **IMPORTANT:** For Lab ONLY, you may need to reboot your device after creating a default gateway. Apply and save your configuration.

 TIP: If messages not visible, try turning ON message display log file

- **/ (CLI) /oper/displog ena**

c. Service Status View

d. Test that web servers are operating (are UP).

 TIP: If messages not visible, try turning ON message display log

- **/ (CLI) /oper/displog ena**

### 3. Export Configuration.

 **IMPORTANT:** At export, always "Include Private Keys" = YES so the configuration can be imported later.

- a. May use CLI command to export: name file STANDARD SETUP.
  - i. Use CLI "put config" command and TFTP server.
  - ii. Use IP address of the Workstation of the management network = 10.10.242.2##.
-  **IMPORTANT:** Reconnect to your Team-PC to see that your STANDARD SETUP file was exported there.
- b. May use web-GUI to export: name file STANDARD SETUP.
  - i. Go to *Configuration > System > Config Mgmt*

### 4. Reset (reboot) Alteon to factory default.

 **IMPORTANT:** Access Alteon console port. Login username / password = admin.

 **IMPORTANT:** Always "Keep Management Network (port)" = YES so you don't have to reconfigure it after reboot is finished.

- a. **After reboot**, labs set TFTP to use management port.
    - i. Use IP Address of Manaement Workstation (Team PC) as 10.10.242.2##
  -  **TIP:** Before you can configure a static address, DHCP must be disabled.
  -  **TIP:** APPLY and SAVE to save changes.
  - b. **After reboot**, enable remote access to management port. Labs enable SNMP.
-  **NOTE:** Radware Labs use AlteonOS v32.+ -- which,by default, ENABLES remote access via SSH and HTTPS. *If your business-setting Alteon uses OSv30.0 or older, you must manually enable SSH / HTTPS separately.*

## 5. Verify configuration: generate test-traffic to your servers (VIP).

 **IMPORTANT:** You will need to configure the VIP to your lab server group. This is your Team##. Use to generate test-traffic within the lab to validate your lab configuration

a. Connect to your (VIP) server(s) from your local computer (directly) by browsing to <http://<LabURL>:24##>.

b. If you cannot connect to your server(s) directly, use VNC Viewer to connect to Team-PC. Then (indirectly) browse to your VIP to connect.

c. Accept Radware as a secure site --add exception.

 **NOTE:** Look for a response that you reached Server1 or Server2. Open a new browser window to see load balancing working.

## 6. View statistics on your virtual server connection.

a. Generate additional test-traffic to servers and view changes in virtual server statistics.

i. Open new browser window to your VIP several times to generate test-traffic.

ii. Return to the Alteon CLI and notice changes to the Alteon statistics.

 **TIP:** In the Alteon CLI, press the up-arrow key to repeat previous command.

b. View statistics on your virtual server connection -- then clear statistics.

c. Clear statistics on SLB table; then repeat Stats view

## 7. Enable Application Trace Log for SSL.

☐ TIP: Application services tracelogging may cause performance impact on Alteon traffic processing capabilities. Be sure to disable when done.

- a. Connect to the page using HTTPS.

## 8. Import configuration.

- a. Check differences between the configurations.

☐ TIP: Use CLI `diff`

- b. Import (`get`) configuration.

☐ TIP: Remember to APPLY and SAVE changes.

## Lab Topology - Alteon VA (printable)

**Remote Lab – Alteon VA**

**Lab Connection Information**

USA	njlab1.radware.net
Germany	delab1.radware.net
Japan	jplab1.radware.net

For VNC display select **FULL** color

**Remote-Client**  
VNC: 22\_\_\_\_\_  
Password: radware

**Management port:**  
Remote Serial (VNC): 25\_\_\_\_\_(A)  
Remote Secure-SSH: 26\_\_\_\_\_(A)  
Remote Secure-WBM: 27\_\_\_\_\_(A)

**Load Balancing:**  
Remote VIP port 80: 24\_\_\_\_\_  
Remote VIP port 443: 23\_\_\_\_\_

**APSolute Vision**  
<https://njvision1.radware.net>  
<https://devision1.radware.net>  
<https://jpvision1.radware.net>  
Username: AL-Team\_\_\_\_\_  
Password: radware

**Alteon A Information**

MNG	10.10.242.____/21
MNG-GW	10.10.240.1

**Ext. Client network**  
port 1 → Vlan 11  
if-1 = 192.168.175.\_\_\_\_/24 Vlan 11

**Server network**  
port 2 → Vlan 14  
if-2 = 10.200.\_\_\_\_\_.\_\_\_\_/24 Vlan 14

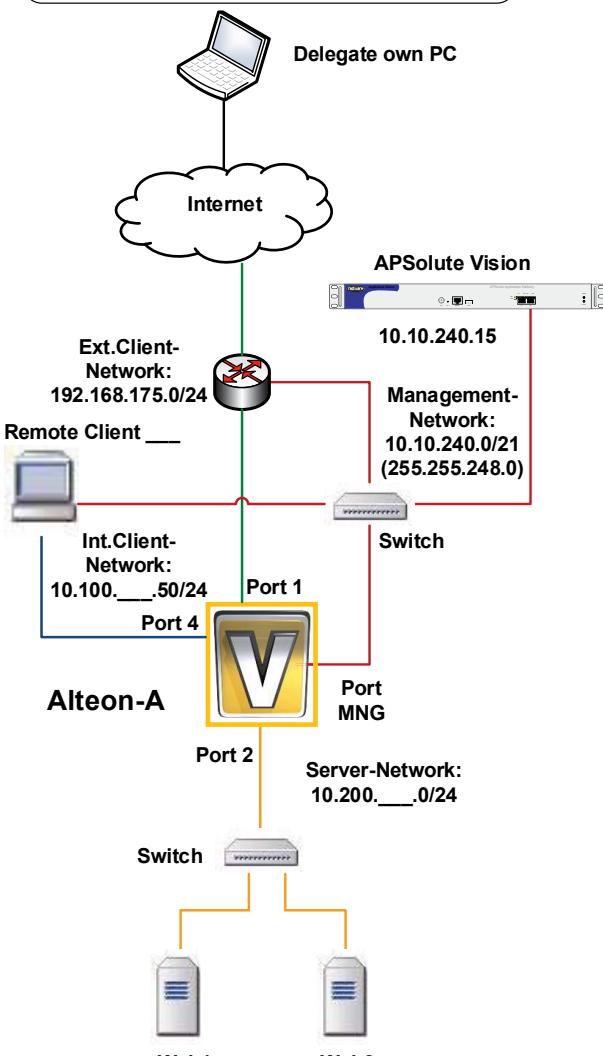
**Int. Client network**  
port 4 → Vlan 24  
if-4 = 10.100.\_\_\_\_.1 /24 Vlan 24

**Gateway 1** = 192.168.175.254

**Load Balancing**  
PIP on port 1: 10.200.\_\_\_\_\_.70  
VIP = 192.168.175.\_\_\_\_\_  
Web1 = 10.200.\_\_\_\_\_.100  
Web2 = 10.200.\_\_\_\_\_.200

**\_\_\_ = team number**

Please put in your Team Number in the Blank fields



## Lab Topology - Alteon HA (printable)

**Remote Lab – Alteon VA - HA**

**Lab Connection Information**

USA	njlab1.radware.net
Germany	delab1.radware.net
Japan	jplab1.radware.net

For VNC display select **FULL** color

**Remote-Client**  
VNC: 22\_\_\_\_\_  
Password: radware

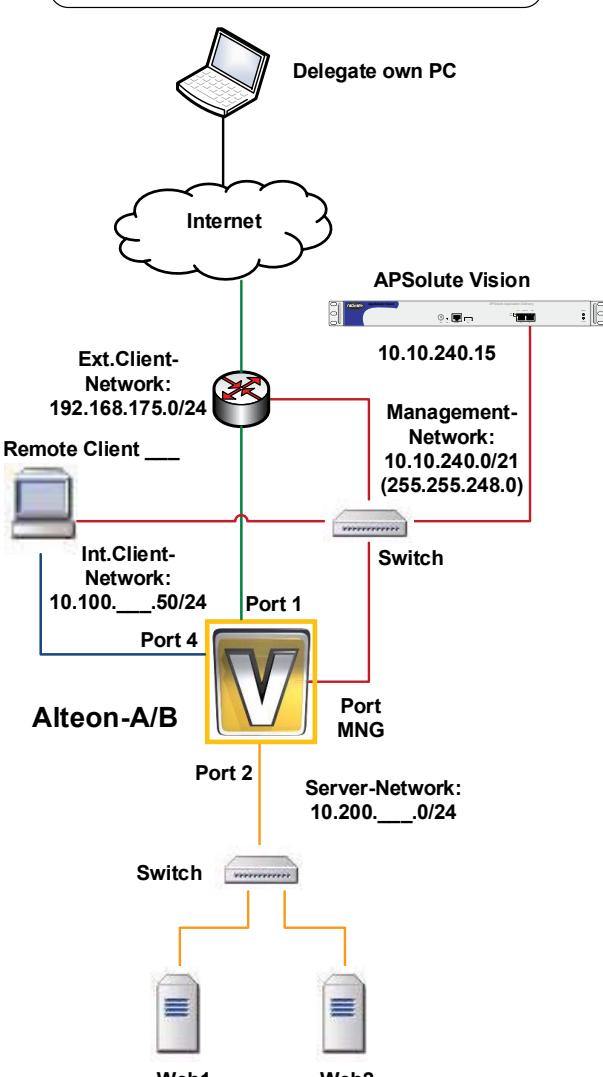
**Management port:**  
Remote Serial (VNC): 25\_\_\_\_\_(A) 250\_\_\_\_\_(B)  
Remote Secure-SSH: 26\_\_\_\_\_(A) 260\_\_\_\_\_(B)  
Remote SecureWBM: 27\_\_\_\_\_(A) 270\_\_\_\_\_(B)

**Load Balancing:**  
Remote VIP port 80: 24\_\_\_\_\_  
Remote VIP port 443: 23\_\_\_\_\_

**APSolute Vision**  
<https://njvision1.radware.net>  
<https://devision1.radware.net>  
<https://jvision1.radware.net>  
Username: AL-Team\_\_\_\_\_  
Password: radware

\_\_\_\_ = team number

Please put in your Team Number in the Blank fields



**Alteon A Information**

MNG	10.10.242.____/21
MNG-GW	10.10.240.1

**External Client network**  
port 1 → Vlan 11  
if-1 = 192.168.175.\_\_\_\_/24 Vlan 11  
Peer IP = 192.168.175.\_\_\_\_/24  
Gateway 1 = 192.168.175.254

**Server network**  
port 2 → Vlan 14 →  
if-2 = 10.200.\_\_\_\_.254 /24 Vlan 14  
Peer IP = 10.200.\_\_\_\_.253 /24

**Internal Client network**  
port 4 → Vlan 24  
if-4 = 10.100.\_\_\_\_.254 /24 Vlan 24  
Peer IP = 10.100.\_\_\_\_.253 /24

**Floating IP Addresses**  
192 . 168 . 175 . \_\_\_\_  
10 . 200 . \_\_\_\_ . \_\_\_\_  
10 . 100 . \_\_\_\_ . 1

**Load Balancing**  
PIP = 10.200.\_\_\_\_.70  
VIP = 192.168.175.\_\_\_\_  
Web1 = 10.200.\_\_\_\_.100  
Web2 = 10.200.\_\_\_\_.200

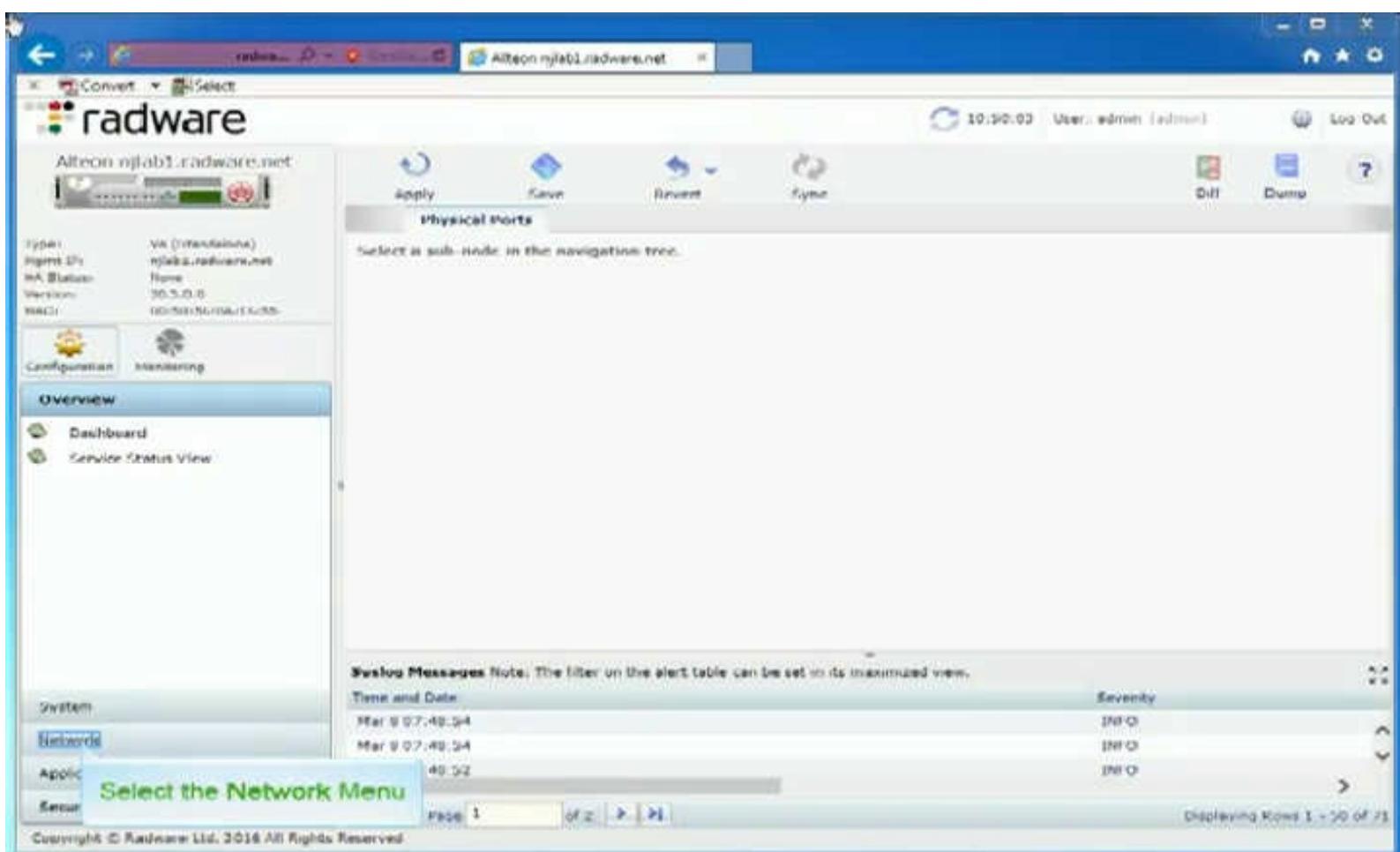
**Alteon B Information**

MNG = 10.10.242.\_\_\_\_/21

IF ID	IP Address	VLAN ID
1	192.168.175.____/24	11
2	10.200.____.253 /24	14
4	10.100.____.253 /24	24

# VIDEO DEMONSTRATION

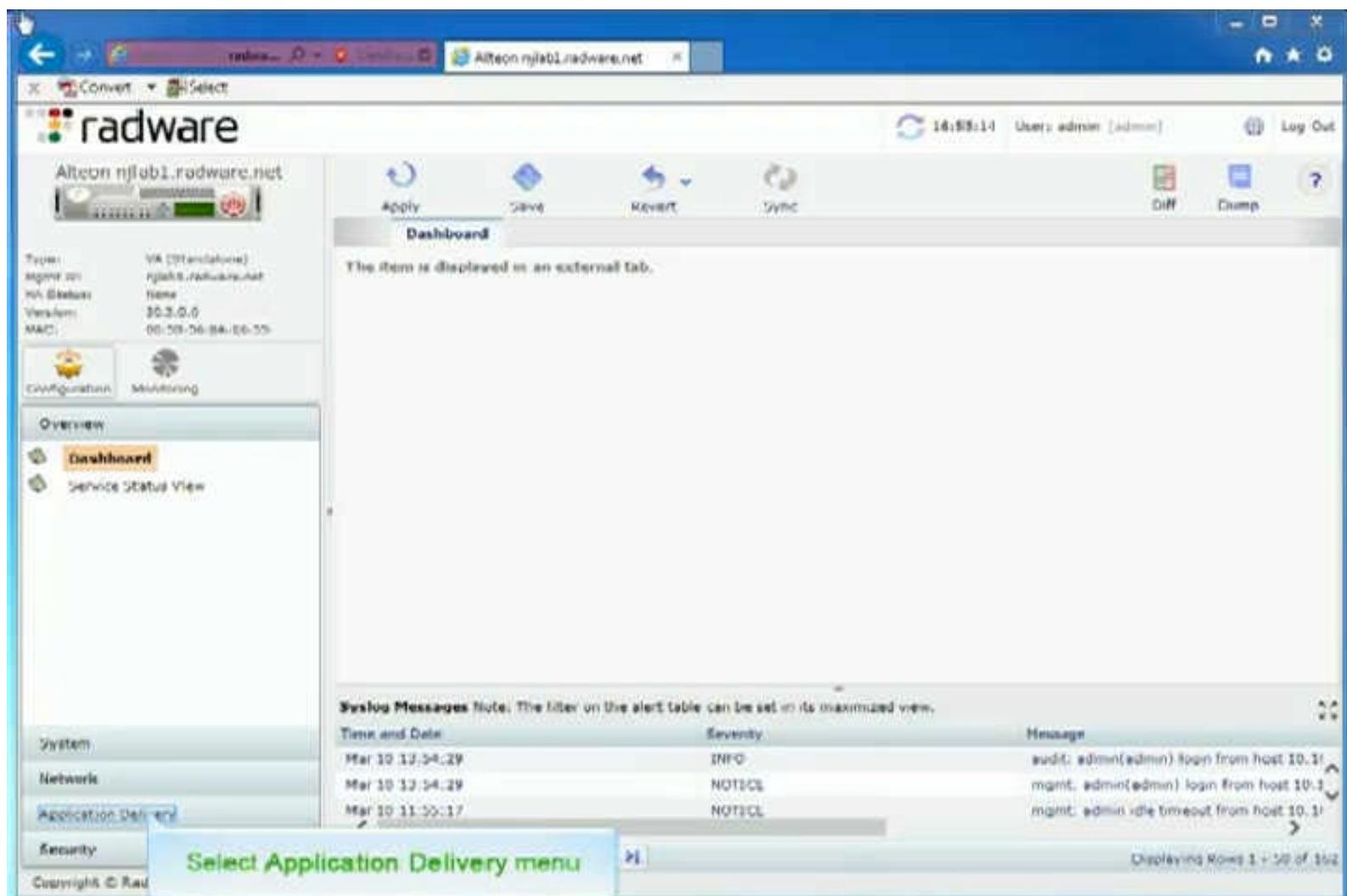
## Create VLAN using Web GUI



The screenshot shows the Alteon Web GUI interface. The title bar indicates the URL is `Alteon n1lab1.radware.net`. The top navigation bar includes links for 'Convert' and 'Select', the Radware logo, and user information ('User: admin [admin]'). The main menu on the left has sections for 'Configuration' and 'Monitoring', with 'Overview' currently selected. Under 'Overview', there are links for 'Dashboard' and 'Service Status View'. The central content area is titled 'Physical Ports' with a sub-instruction 'Select as sub-node in the navigation tree.' Below this, there is a table titled 'Alert Log Messages' with a note: 'Note: The filter on the alert table can be set in its maximized view.' The table has columns for 'Time and Date', 'Message', and 'Severity'. It lists three entries: 'Mar 9 07:48:54', 'Mar 9 07:48:54', and '48:52'. The bottom of the screen displays a footer with the text 'Select the Network Menu' and 'Copyright © Radware Ltd. 2016 All Rights Reserved'.

# VIDEO DEMONSTRATION

## Create Server Group using Web GUI



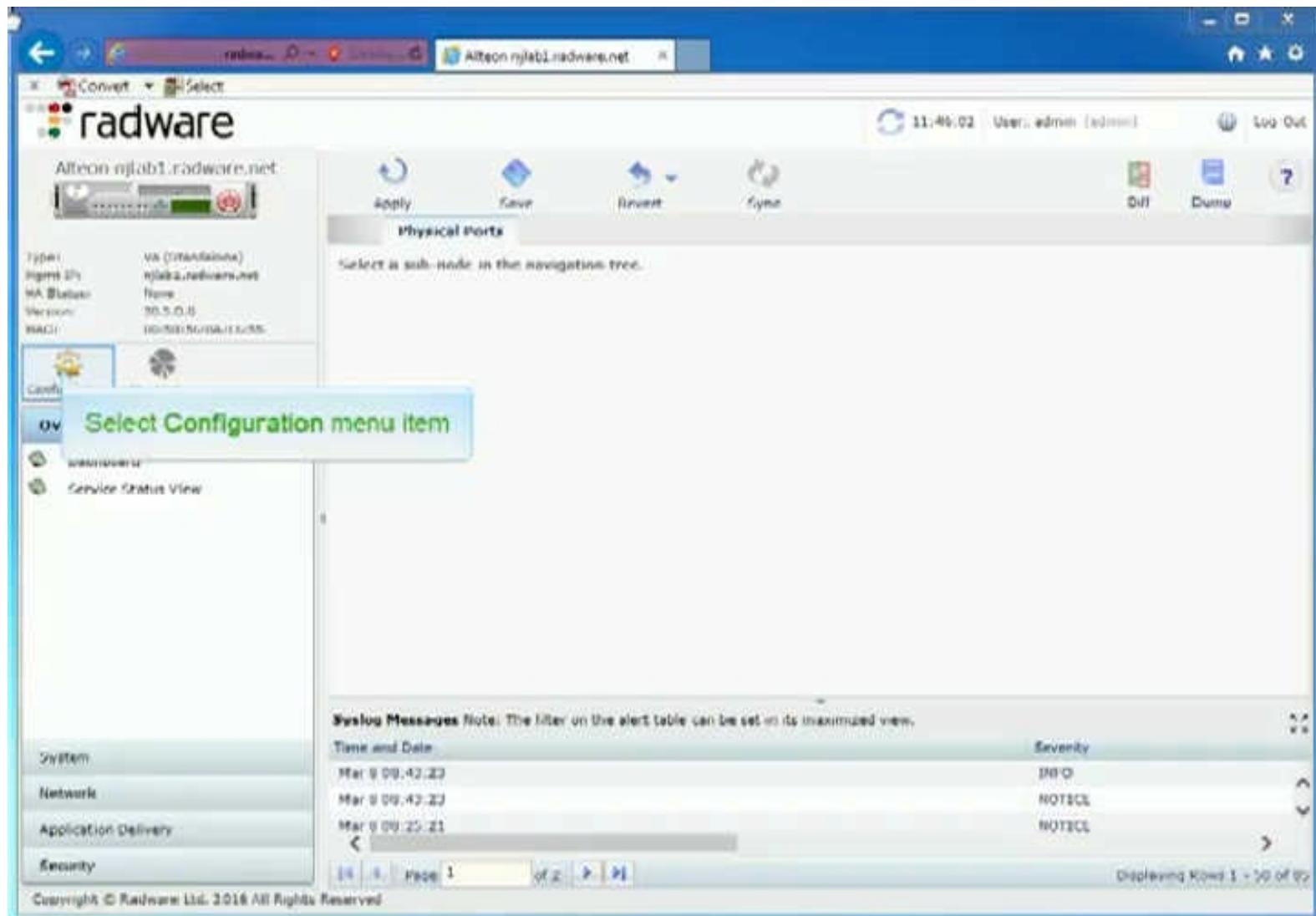
The screenshot shows the Alteon Web GUI interface. At the top, there's a browser-like header with tabs for 'Convert' and 'Select'. Below it is the main dashboard area. On the left, a sidebar lists 'Overview', 'Dashboard' (which is selected), and 'Service Status View'. The main content area displays system status with tabs for 'Apply', 'Save', 'Revert', and 'Sync'. It also shows a message: 'The item is displayed in an external tab.' Below this is a 'System Log' section with a table of log messages:

System Log			
Time and Date	Severity	Message	
Mar 10 12:58:29	INFO	audit: admin(admin) login from host 10.31	
Mar 10 12:54:29	NOTICE	mgtnt: admin(admin) login from host 10.31	
Mar 10 11:55:17	NOTICE	mgtnt: admin idle timeout from host 10.31	

At the bottom of the dashboard, there's a green button labeled 'Select Application Delivery menu'.

# VIDEO DEMONSTRATION

## Add IP Interface using Web GUI



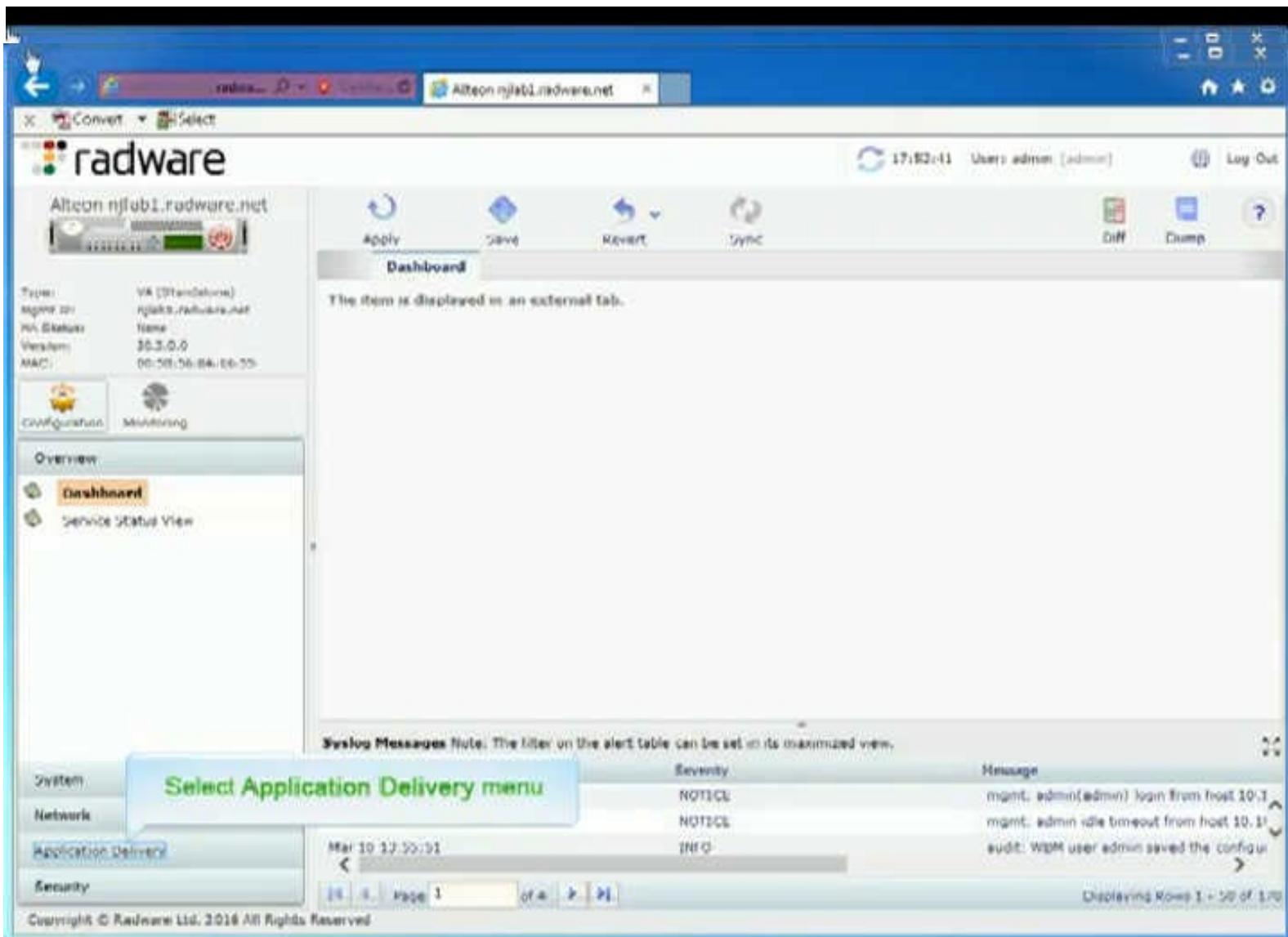
The screenshot shows the Alteon Web GUI interface. The title bar indicates the URL is "Alteon-njlab1.radware.net". The top navigation bar includes "Convert", "Select", "radware" logo, "Logout", and "Log Out". The main menu on the left is expanded to show "Select Configuration menu item". Sub-options under "Select Configuration menu item" include "System", "Network", "Application Delivery", and "Security". The "System" option is currently selected. The central pane displays the "Physical Ports" configuration page with the message "Select a sub-node in the navigation tree." Below this is a "Syslog Messages" table with the following data:

Time and Date	Severity
Mar 9 09:42:23	INFO
Mar 9 09:42:23	NOTICE
Mar 9 09:25:21	NOTICE

At the bottom of the screen, a footer bar displays "Copyright © Radware Ltd. 2016 All Rights Reserved" and "Displaying Row 1 - 50 of 99".

# VIDEO DEMONSTRATION

## Create Virtual Server using Web GUI



The screenshot shows the Alteon Web GUI interface. The top navigation bar includes a back button, forward button, refresh button, and a search bar containing "Alteon nJLB1.radware.net". The top right corner shows the date and time "17:52:11" and the user "admin (admin)". There are "Log Out" and "Diff" buttons.

The main dashboard area has several buttons: "Apply", "Save", "Revert", and "Sync". Below them is a message: "The item is displayed in an external tab." On the far right of the dashboard are "Diff" and "Compare" buttons.

The left sidebar contains a "Configuration" section with "Type: VR (Standard)", "IP: 192.168.1.100", "Name: Name", "Version: 3.0.0.0", and "MAC: 00:58:56:84:1E:55". It also includes "Monitoring" and "Overview" sections, with "Dashboard" currently selected.

A tooltip "Select Application Delivery menu" is displayed over the "Application Delivery" tab in the sidebar.

The bottom right corner shows a log messages table with columns "Severity", "Message", and a scrollable list of entries:

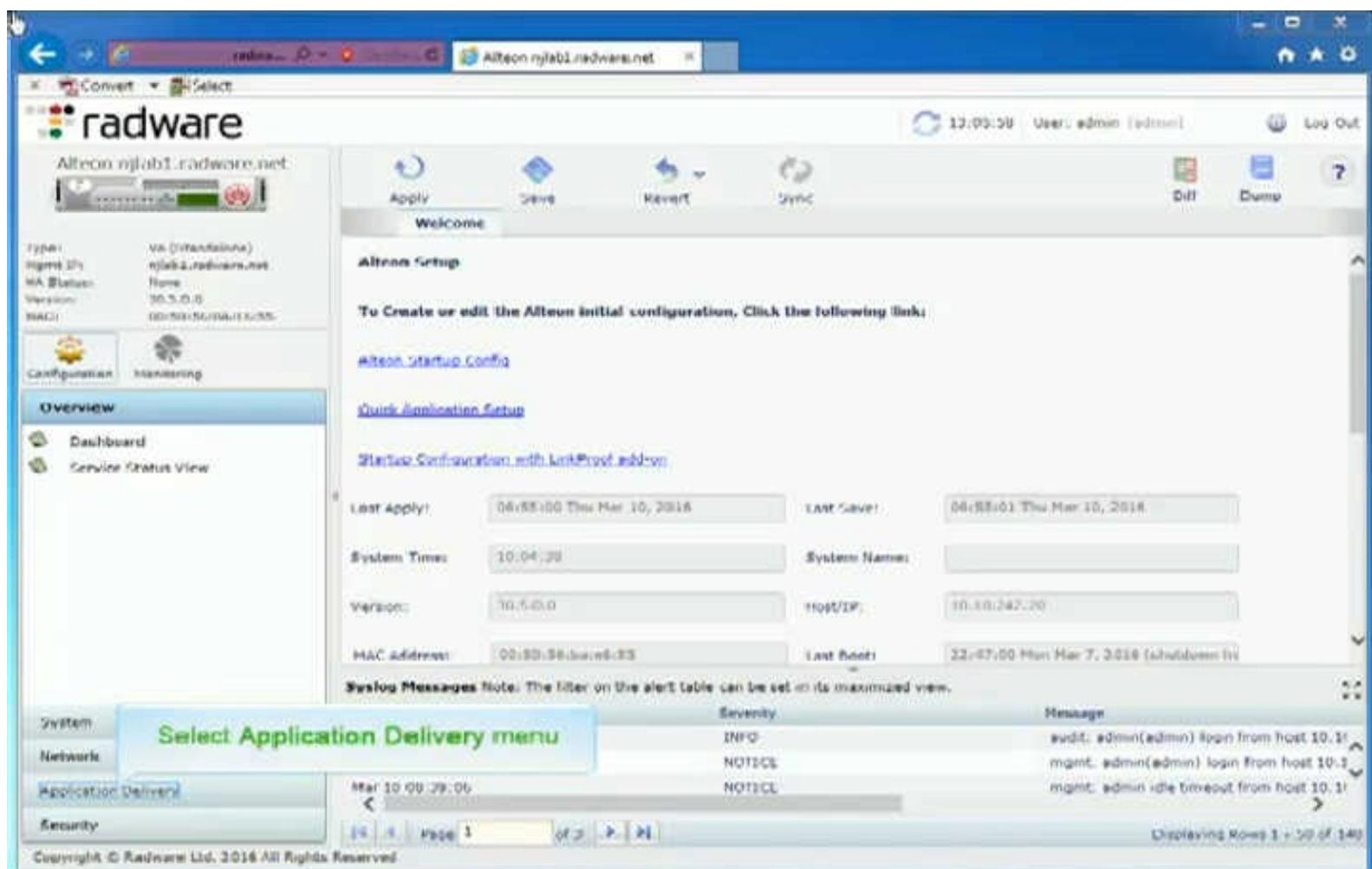
Severity	Message
NOTICE	mgmt. admin(admin) login from host 10.1.1.1
NOTICE	mgmt. admin idle timeout from host 10.1.1.1
INFO	audit: WBM user admin saved the configuration

Page navigation controls at the bottom include "Page 1" and "of 1" with arrows, and a note "Displaying Rows 1 - 10 of 170".

Copyright © Radware Ltd. 2016 All Rights Reserved

# VIDEO DEMONSTRATION

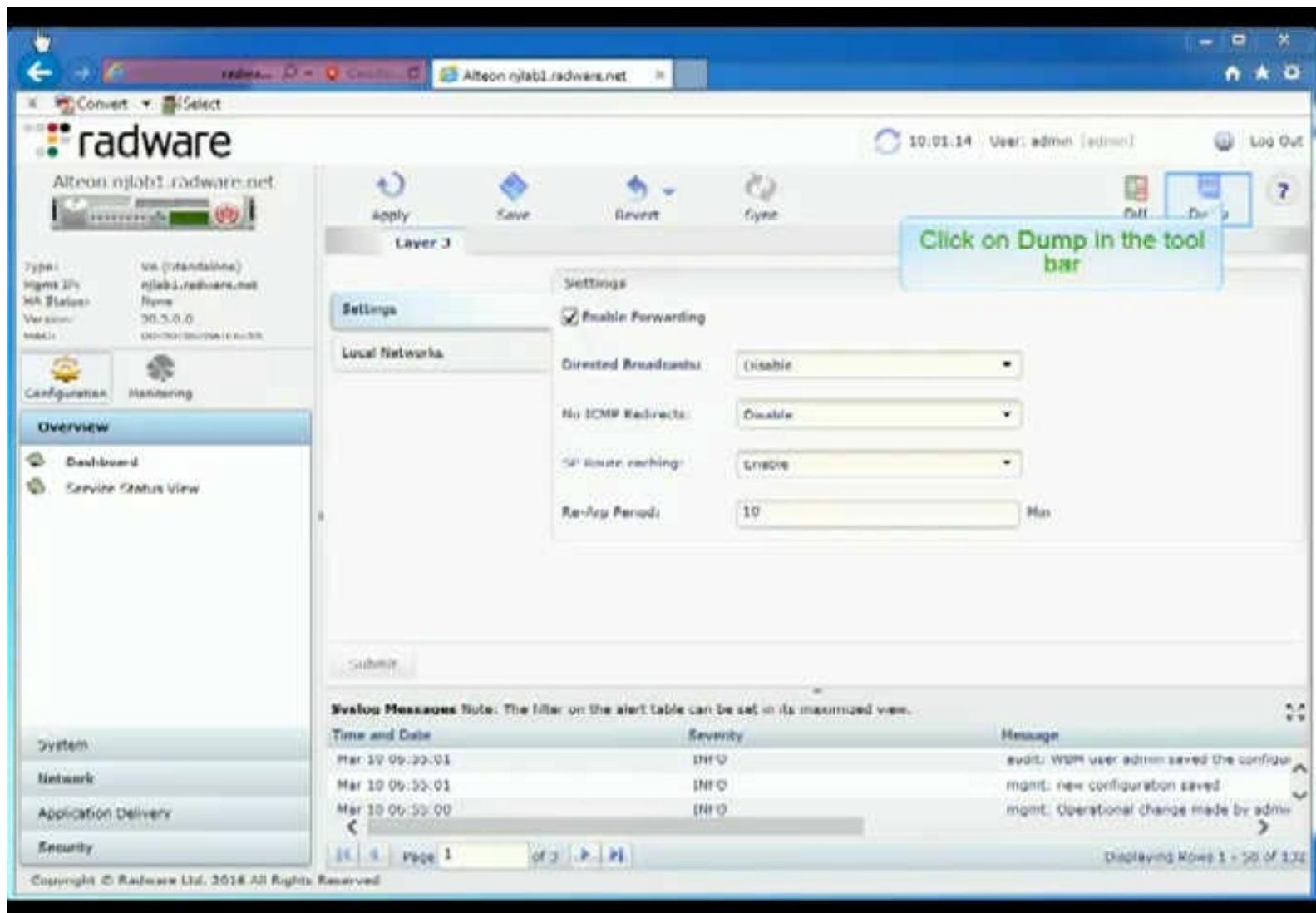
## Define Real Servers using Web GUI



The screenshot shows the Alteon Web GUI interface. The top navigation bar includes a back button, forward button, refresh button, and a search bar with the URL "Alteon mylab1.radware.net". The top right corner shows the time "12:03:58", user "admin (admin)", and a "Log Out" link. Below the header is a toolbar with "Apply", "Save", "Revert", "Sync", "Diff", "Dump", and a help icon. The main content area is titled "Welcome" and contains sections for "Alteon Setup" and "System Configuration with WebProv add-on". It displays system information such as Last Apply (06:58:00 Thu Mar 10, 2016), Last Save (06:58:01 Thu Mar 10, 2016), System Time (10:04:29), System Name (empty), Version (10.5.0.0), Host IP (10.10.242.20), MAC address (00:BD:3B:0A:e6:33), and Last Boot (22:07:00 Mon Mar 7, 2016 (idleboot)). A "MsgLog Messages" section shows three log entries: "audit: admin(admin) login from host 10.31", "mgmt: admin(admin) login from host 10.31", and "mgmt: admin idle timeout from host 10.31". The bottom of the page features a footer with copyright information: "Copyright © Radware Ltd. 2016 All Rights Reserved" and a page navigation bar with "Page 1" and "of 2". A green callout box highlights the "Select Application Delivery menu" link.

# VIDEO DEMONSTRATION

## Save Configuration using Web GUI



The screenshot shows the Alteon Web GUI interface. On the left, there's a navigation sidebar with sections like Overview, Configuration, Monitoring, System, Network, Application Delivery, and Security. The main content area is titled 'Layer 3' and contains a 'Settings' tab. Under 'Settings', there are several configuration options: 'Enable Forwarding' (checkbox checked), 'Directed Broadcasts' (dropdown set to 'Disable'), 'No ICMP Redirects' (dropdown set to 'Disable'), 'IP Route caching' (dropdown set to 'Enable'), and 'Re-Avg Period' (dropdown set to '10'). At the top right of the main area, there are buttons for 'Apply', 'Save', 'Revert', and 'Sync'. To the right of these buttons is a timestamp '10.01.14 User: admin [admin]' and a 'Log Out' link. A callout box with the text 'Click on Dump in the tool bar' points to the 'Dump' button in the toolbar at the top of the window. At the bottom of the screen, there's a 'System Messages' section showing log entries:

Time and Date	Severity	Message
Mar 10 09:20:01	INFO	audit: WSM user admin saved the config
Mar 10 09:20:01	INFO	mgmt: new configuration saved
Mar 10 09:20:00	INFO	mgmt: Operational change made by admin

Page 1 of 2 > >> Displaying Rows 1 - 50 of 324

## Configuration Files (to copy/paste)

### HIGH AVAILABILITY CONFIGURATION

#### Device A

```
/c/l3/if 1/addr 192.168.175.2##/mask 255.255.255.0/ena/vlan 11/peer 192.168.175.1##  
/c/l3/if 2/addr 10.200.##.254/mask 255.255.255.0/ena/vlan 14/peer 10.200.##.253  
/c/l3/if 4/addr 10.100.##.254/mask 255.255.255.0/ena/vlan 24/peer 10.100.##.253  
/c/l3/gw 1/addr 192.168.175.254/ena  
/c/l3/ha/switch/failback always/pref active  
/c/slb/sync/peer 1/ena/addr 192.168.175.2##
```

#### Device B

```
/c/l3/if 1/addr 192.168.175.1##/mask 255.255.255.0/ena/vlan 11/peer 192.168.175.1##  
/c/l3/if 2/addr 10.200.##.253/mask 255.255.255.0/ena/vlan 14/peer 10.200.##.254  
/c/l3/if 4/addr 10.100.##.253/mask 255.255.255.0/ena/vlan 24/peer 10.100.##.254  
/c/l3/gw 1/addr 192.168.175.254/ena  
/c/l3/ha/switch/failback always/pref standby  
/c/slb/sync/peer 1/ena/addr 192.168.175.1##
```

#### Devices A&B

```
/c/l3/ha/floatip 1/if 1/addr 192.168.175.##/ena  
/c/l3/ha/floatip 2/if 2/addr 10.200.##.##/ena  
/c/l3/ha/floatip 4/if 4/addr 10.100.##.1/ena  
/c/slb/real Server1/rip 10.200.##.100/ena  
/c/slb/real Server2/rip 10.200.##.200/ena  
/c/slb/group 1/add Server1/add Server2  
/c/slb/virt 1/vip 192.168.175.%%/ena/service 80/group 1/pip	mode address/addr v4 10.200.##.69 255.255.255.255  
/c/l3/hamode switch  
/c/l3/ha/switch/add 1/add 2/add 4
```



TIP: Go back to Lab Manual